Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Prototipe Pengamanan RSA untuk Dokumen Borang Program Studi

Aji Setiawan, Nenda Fitriana, Mitchell Marcel

Darma Persada University, Jl. Raden Inten II, Kota Jakarta Timur, 13450

KEYWORDS

RSA Algorithm, Cryptography, UML

CORRESPONDENCE

Phone: +62 87885025203

E-mail: aji_setiawan@ft.unsada.ac.id

A B S T R A C T

Cryptography is the science or art of securing messages and is done by a cryptographer. The data that is guaranteed includes several aspects such as aspects of messages security such as confidentiality, data integrity, and authentication. One of the cryptographic algorithms that are often used in securing data is the RSA algorithm. RSA stands for the names of the founders of this algorithm, namely Ron, Shamir, and Adleman. RSA is an algorithm that uses the concept of public-key cryptography (the asymmetry/key used to encrypt is different from the one used to decrypt). The importance of information causes the desired information to be accessed only by certain people. The unwanted fall of information to other parties can be detrimental to the party holding the data. This study discusses the use of the RSA algorithm to build a document security system prototype. The study results explain that the RSA algorithm can be applied to secure important documents based on case studies at universities.

ABSTRAK

Cryptography adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh cryptographer. data-data yang diamankan meliputi beberapa aspek seperti aspek keamanan pesan seperti kerahasiaan, integritas data, serta otentikasi. Salah satu algoritma kriptografi yang sering digunakan dalam proses pengamanan data yaitu algoritma RSA. RSA adalah salah satu algoritma yang menggunakan konsep kriptografi kunci publik (asimetri / kunci yang digunakan untuk mengenkripsi berbeda dengan yang digunakan untuk mendekripsi). Penelitian ini membahas penggunaan algortima RSA untuk membangun sebuah prototipe sistem pengamanan dokumen pada jurusan teknologi informasi. Hasil penelitian menerangkan bahwa algoritma RSA dapat diterapkan untuk pengamanan dokumen penting berdasarkan studi kasus di universitas.

PENDAHULUAN

Era teknologi yang berkembang sangat cepat saat ini mengharuskan setiap organisasi dengan latar belakang *profit oriented* maupun sosial harus ikut bergerak berdampingan dengan teknologi. Salah satunya terkait pentingnya sebuah informasi atau data, sangat pentingnya sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu saja atau dengan kata lain dapat di istilahkan dengan *private area*. Berdasarkan latar belakang tersebut keamanan dari sistem informasi yang digunakan haruslah terjamin dalam batas yang dapat diterima. Privasi atau kerahasiaan merupakan bagian yang sangat penting untuk mencegah terbukanya akses terhadap data-data penting atau sensitif oleh orang-orang yang tidak berhak *(anonymous)*.

Beberapa cara yang dapat dilakukan untuk mencegah pencurian data yaitu dengan cara mengamankan data dengan pendekatan kriptografi pada sebuah system. Perlindungan dan keamanan terhadap kerahasiaan data privasi dengan menggunakan pendekatan kriptografi saat ini semakin meningkat, dimana salah satu caranya dengan penyandian data atau enkripsi. Ada beberapa algoritma enkripsi yang biasa digunakan, salah satunya adalah RSA (Rivest-Shamir-Adleman). RSA merupakan algoritma yang cocok untuk digital signature seperti halnya enkripsi [1], dan salah satu yang paling maju dalam bidang kriptografi *public key* [2].

Beberapa penelitian RSA dilakukan diantaranya Gunawan [3], menggunakan kombinasi algoritma Caesar cipher dan RSA untuk pengamanan dokumen dan menghasilkan kesimpulan bahwa tingkat pengamanan file dokumen dan pesan teks bisa lebih terjaga keaslian datanya. Susanto dan Trisusilo [4], mengaplikasikan penggunaan RSA pada sistem penjualan yang akan dibangun, hasilnya data dalam database khususnya terkait angka penjualan tidak dimengerti oleh pihak yang tidak berkepentingan.

METODOLOGI

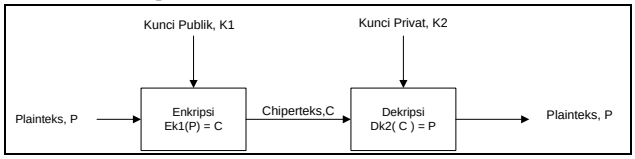
Metode penelitian yang dilakukan berdasarkan hasil wawancara dan data terkait jenis dokumen yang dianggap penting.

https://doi.org/10.30743/infotekjar.v6i2.4263

Attribution-NonCommercial 4.0 International. Some rights reserved

Kunjungan ke lokasi penelitian untuk mendapatkan data primer yang digunakan dalam mengembangkan keamanan dengan RSA untuk menguji keamanan dokumen. Pengembangan sistem algoritma RSA terlihat pada gambar 1 [5].

Algoritma RSA merupakan salah satu algoritma kriptografi kunci publik (public key cryptography) dengan memakai kunci yang berbeda pada saat proses enkripsi dan dekripsi. Penggunaan algoritma RSA masih digunakan secara luas dan salah satu yang paling maju dalam bidang kriptografi public key. Algortima RSA termasuk dalam kategori algoritma asimetris, yaitu kunci yang digunakan pada proses enkripsi berbeda dengan yang digunakan untuk mendekripsi.

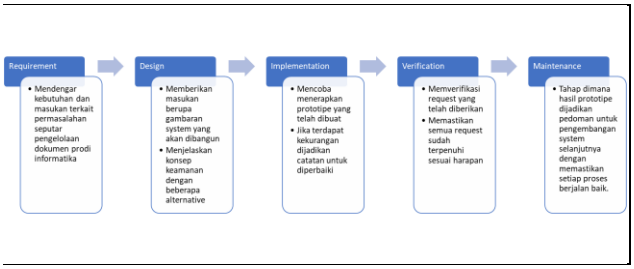


Gambar 1. Skema Algoritma Asimetri (Munir, 2006)

Dalam tahapan perancangan sistem, penelitian ini menggunakan model pengembangan waterfall, penggunaan model ini memiliki keunggulan yaitu pada setiap tahapan dilakukan secara bertahap pada setiap prosesnya, proses bertahap ini dapat mengurangi tingkat kesalahan pengembangan yang lebih kompleks [6]. Metode waterfall (air terjun) memastikan bahwa langkah logis pada setiap proses harus dilakukan sepanjang siklus pengembangan software (SDLC) [6] yang terdiri dari beberapa tahapan penelitian.

1. System Engineering
   Pada tahap ini dijelaskan dan dibuktikan dengan adanya dokumen kebutuhan sistem.
2. Requirement Analysis (Analisa Kebutuhan)
   Pada tahapan ini dilakukan analisa terkait kebutuhan dalam menghasilkan model bisnis yang sesuai harapan.
3. System Design (Desain Sistem)
   Pada tahap ini membuat interface / tampilan layout dari sistem.
4. Coding (Penulisan Kode Program)
   Pada tahapan ini dilakukan pembuatan kode program berdasarkan dari alur design dan kebutuhan dengan tujuan awal membuat sistem keamanan RSA berbasis web.
5. Integration & Testing (Penerapan dan Pengujian Program)
   Tahap ini dilakukan sosialisasi penggunaan aplikasi dan juga pengujian sistem, langkah ini bertujuan agar dapat mengetahui ada atau tidaknya error.
6. Operation & Maintenance (Pemeliharaan)
   Tahap untuk melakukan pemeliharaan untuk menjaga sistem tetap berjalan sebagai mana yang diharapkan.

SDLC dapat digunakan untuk pengembangan web maupun aplikasi mobile seperti yang dilakukan oleh putri [7] yang membangun aplikasi mobile peternakan telur ayam dengan pendekatan SDLC. Penggunaan metode waterfall terhadap pembuatan prototype keamanan dokumen dengan algoritma RSA melalui beberapa tahapan pada gambar 2.



Gambar 2. Proses waterfall sistem keamanan dokumen

HASIL DAN PEMBAHASAN

A. Proses *RSA*

Algoritma Kriptografi RSA menggunakan beberapa persamaan dalam melakukan proses generate key, proses enkripsi dan dekripsi. Pada proses generate key (perubahan kunci) algoritma kriptografi RSA membutuhkan sepasang kunci berpasangan yang buat dengan memilih bilangan prima p dan q, besaran yang digunakan dalam mengenerate kunci RSA diantaranya.

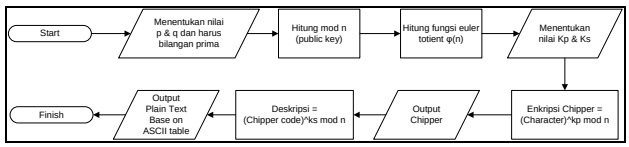
a. p dan q (merupakan bilangan prima)
b. $n = p \times q$
c. Totient(n) = (p - 1) (q – 1)
d. e (Enkripsi key)
e. d (Deskripsi key)
f. m (Plaintext)
g. c (Ciphertext)

Menurut Munir [5] rumus pembuatan algoritma RSA berdasarkan pada persamaan matematika dan teorema Euler sehingga mendapatkan rumus untuk enkripsi. Adapun rumus enkripsi dan deskripsi adalah seperti pada persamaan 1 dan 2.

$$C = M^{e} \bmod n \qquad (1)$$

$$C = M^{d} \bmod n \qquad (2)$$

Keterangan :
C : ciphertext (blok plaintext yang sudah dienkripsi)
M : message (blok pesan yang akan dienkripsi)
e : enciphering
d : deciphering
n : nilai modulus

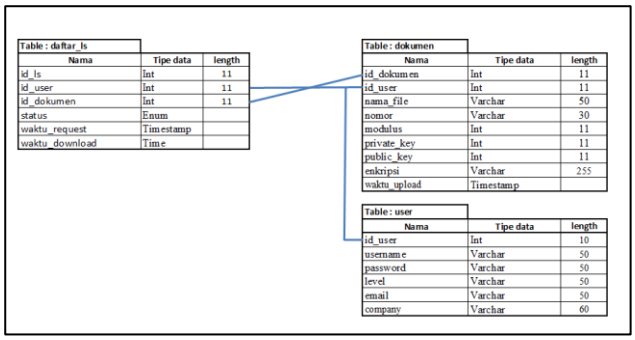


Gambar 3. Proses RSA

B. Sistem dan design software

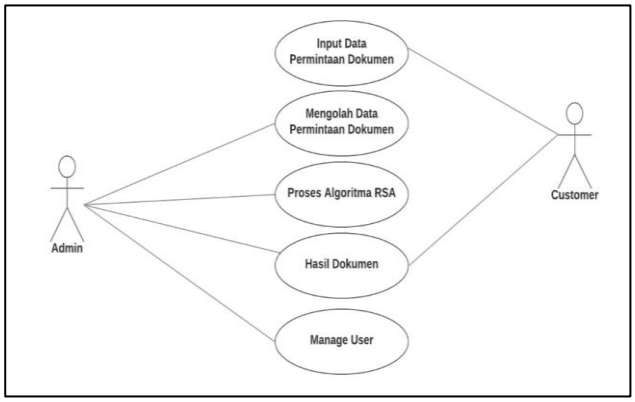
Penggunaan Entity Relational Diagram (ERD) untuk mewakili dekomposisi domain subjek menjadi entitas. ERD merupakan node yang mewakili tipe entitas, dan edge (garis asosiasi) yang menggambarkan hubungan dari setiap entitas [9]. Hasil pembuatan tabel ERD dapat dilihat pada Gambar 4

https://doi.org/10.30743/infotekjar.v6i2.4263



Gambar 4. Entity Relational Diagram

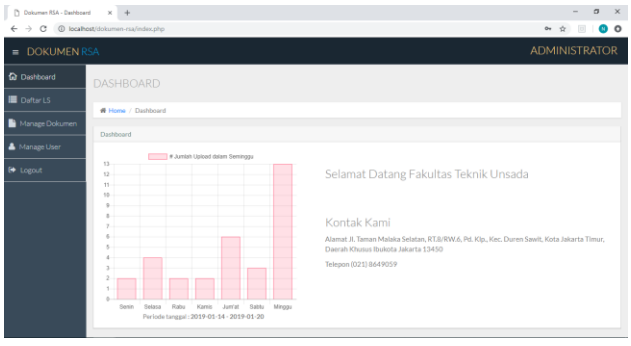
Perancangan dengan UML merupakan bagian dalam tahapan yang disebut proses development system, pada tahap ini bisa digambarkan dengan interaksi antar user dengan sistem yang biasa disebut dengan use case. Use case dari sistem keamanan RSA ini terlihat pada gambar 5.



Gambar 5. Use Case

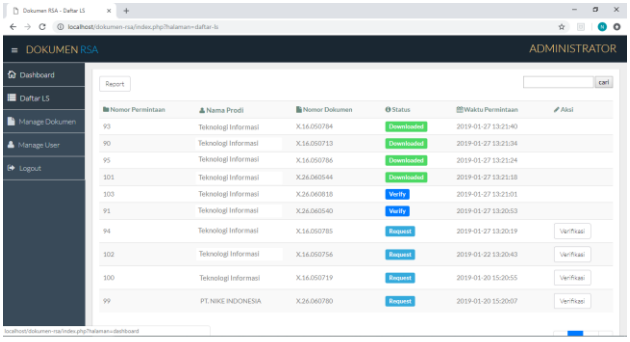
Pada gambar 5 admin dapat mengelola data permintaan dokumen, user, memproses algoritma RSA, dan melihat hasil proses RSA, sedangkan user dapat menginput permintaan dokumen dan melihat dokumen yang sudah di verifikasi admin.

C. Implementasi



Gambar 6. Halaman Dashboard

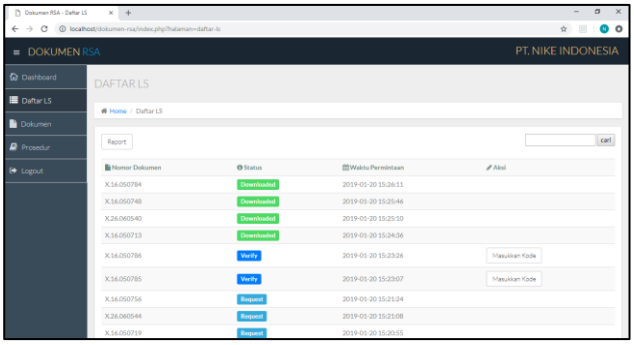
Halaman dashboard admin merupakan tampilan awal setelah admin melakukan login dari sistem keamanan data dokumen dengan Algoritma RSA. Pada halaman dashboard admin berisi halaman mengenai grafik informasi jumlah dokumen yang telah di upload dalam periode satu minggu.



Gambar 7. Halaman permintaan dokumen

Halaman daftar ls admin merupakan halaman yang berfungsi untuk melihat permintaan dokumen ls dari user yang berisi informasi nomor permintaan, nama prodi, nomor dokumen, status, waktu permintaan, dan tombol verifikasi permintaan dari user yang akan muncul jika informasi pada status berisi request, namun jika informasi pada status berisi verify atau downloaded maka tombol verifikasi tidak akan muncul. Selain itu terdapat tombol report yang berfungsi menarik data daftar ls agar menjadi laporan dalam bentuk microsoft excel.

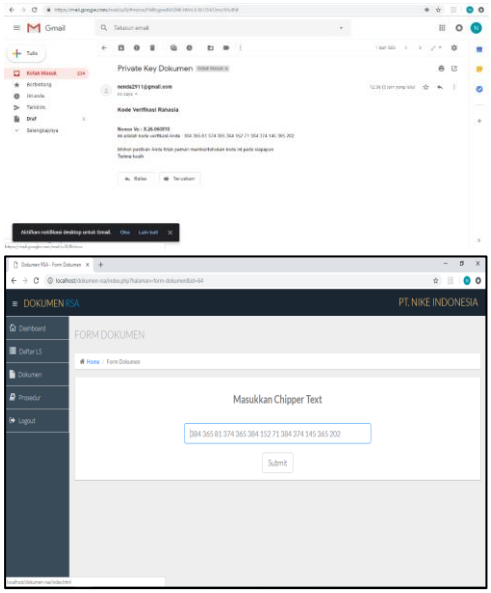
Jika informasi pada status berisi request berarti ada permintaan dokumen dari user dimana terdapat tombol verifikasi yang jika di klik oleh admin maka status akan berubah menjadi verify dan tombol verifikasi akan otomatis hilang. Jika informasi status berisi downloaded berarti user telah berhasil mendownload dokumen tersebut.



Gambar 8. Halaman permintaan user

Halaman daftar ls user merupakan halaman permintaan dokumen ls dari user yang berisi informasi nomor dokumen, status, waktu request, dan tombol masukkan kode yang akan muncul jika informasi pada status berisi verify, namun jika informasi pada status berisi request atau downloaded maka tombol masukkan kode tidak akan muncul. Selain itu terdapat tombol report yang berfungsi menarik data daftar ls agar menjadi laporan dalam bentuk microsoft excel.

Jika informasi pada status berisi verify berarti admin telah memverifikasi permintaan dokumen dari user dan otomatis kode akan terkirim melalui email user dan kode tersebut harus di input oleh user melalui tombol masukkan kode.



Gambar 9. Proses pengiriman kode RSA

D. Evaluasi

Pengujian hasil ini dilakukan dengan cara menganalisis hasil wawancara tentang aplikasi keamanan data pada dokumen dengan algoritma RSA. Dari hasil wawancara tersebut secara umum responden berpendapat baik dalam penilaian aplikasi keamanan data pada dokumen dengan algoritma RSA. Analisis dari hasil penilaian pembuatan aplikasi ini bertujuan untuk mendapatkan data dan pendapat dari pihak penggunan aplikasi keamanan data pada dokumen dengan algoritma RSA yang terdiri dari beberapa bahasan utama :

1. Fungsionalitas, memperlihatkan kinerja dan fungsi kegunaan dari aplikasi keamanan data pada dokumen dengan algoritma RSA.
2. Tampilan, yang memperlihatkan visualisasi aplikasi keamanan data pada dokumen import dengan algoritma RSA.
3. Informatif, memperlihatkan ketersediaan konten yang sesuai dengan informasi yang ingin di dapatkan.

TABLE 1. REKAPITULASI HASIL KUESIONER

Pertanyaan	Penilaian				
	KS	K	C	B	BS
Tampilan keseluruhan aplikasi	0%	10%	40%	50%	0%
Pemilihan warna tema aplikasi	0%	30%	30%	40%	0%
Tepat dalam pengaturan tata letak aplikasi	0%	20%	20%	40%	20%
Kelengkapan fungsi-fungsi yang dibutuhkan dalam aplikasi	0%	20%	50%	30%	0%
Fungsi-fungsi aplikasi sesuai yang di inginkan	0%	0%	60%	40%	0%
Semua fungsi-fungsi dapat digunakan dengan baik	0%	0%	20%	70%	10%
Kemudahan dalam menggunakan aplikasi	0%	0%	20%	80%	0%
Kelengkapan informasi	0%	0%	40%	30%	30%
Pendapat keseluruhan tentang aplikasi	0%	20%	40%	40%	0%

Keterangan : KS (Kurang Sekali), K (Kurang), C (Cukup), B (Baik), BS (Baik Sekali)

TABLE 2. REKAPITULASI BERDASARKAN VARIABEL

Pertanyaan	Penilaian				
	KS	K	C	B	BS
Tampilan	0%	20%	30%	43%	7%
Fungsionalitas	0%	7%	43%	47%	3%
Informatif	0%	7%	33%	50%	0%

Keterangan : KS (Kurang Sekali), K (Kurang), C (Cukup), B (Baik), BS (Baik Sekali)

KESIMPULAN

Kesimpulan penelitian berdasarkan hasil wawancara yang dilakukan dengan responden, menyimpulkan bahwa hasil implementasi aplikasi keamanan data pada dokumen dengan algoritma RSA dinilai baik dan berguna dalam pengamanan dokumen. Penilaian responden terhadap prototipe yang dibangun menyebutkan bahwa secara tampilan sudah cukup baik dengan presentase 73%, fungsionalitas sistem sebesar 90% dan variable informatif sebesar 83%.

Saran yang dapat diberikan untuk penelitian selanjutnya yaitu penggunaan metode algoritma RSA bukan satu-satunya metode keamanan data dokumen, penggunaan metode lain seperti Shamir Secret Sharing, Diffie - Hellman Key Exchange, AES (Advanced Encryption Standard) dapat dicoba agar mendapatkan hasil perbandingan guna mendukung keamanan data yang lebih baik dan efektif.

REFERENCE

[1] Z. L. Ping, S. Q. Liang, and L. X. Liang, "RSA encryption and digital signature," in *Proceedings - 2011 International Conference on Computational and Information Sciences, ICCIS 2011*, 2011.

[2] L. S. Reddy, "RM- RSA algorithm," *J. Discret. Math. Sci. Cryptogr.*, 2020.

[3] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, 2018.

[4] S. Susanto and A. A. Trisusilo, "PENERAPAN ALGORITMA ASIMETRIS RSA UNTUK KEAMANAN DATA PADA APLIKASI PENJUALAN CV. SINERGI COMPUTER LUBUKLINGGAU BERBASIS WEB," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, 2018.

[5] I. R. Munir, "Algoritma RSA dan ElGamal,"

https://doi.org/10.30743/infotekjar.v6i2.4263

Kriptografi, 2010.

[6] A. Powell-Morse, "Waterfall Model: What Is It and When Should You Use It?," *Airbrake*, 2016.

[7] P. Handayani and A. Setiawan, "Perancangan Sistem Informasi Warga Bintara Jaya berbasis Android dengan Waterfall Software Development Life Cycle," *J. Inform. J. Pengemb. IT*, 2019.

[8] Y. Bassil, "A Simulation Model for the Waterfall Software Development Life Cycle," *Int. J. Eng. Technol.*, vol. 2, no. 5, pp. 2049–3444, 2012.

[9] R. J. Wieringa, "Entity-Relationship Diagrams," in *Design Methods for Reactive Systems*, 2007.