Computer Based Information System Journal

ISSN (Print): 2337-8794 | E- ISSN : 2621-5292
web jurnal : http://ejournal.upbatam.ac.id/index.php/cbis

PENGAMANAN RSA UNTUK DOKUMEN BORANG PROGRAM STUDI UNIVERSITAS DARMA PERSADA

Aji Setiawan[1], Nenda Fitriana[2], Mitchell Marchel[3]
[1,2,3]*Program Studi Teknologi Informasi, Universitas Darma Persada, Indonesia.*

INFORMASI ARTIKEL

Diterima Redaksi: 27 Februari 2022
Diterbitkan *Online*: 28 Maret 2022

KATA KUNCI

Cryptography, RSA Algorithm, Document Security System

KORESPONDENSI

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 guaranteed data includes several aspects such as 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/ encryption and decryption process using different key codes). 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 secure essential documents based on university case studies

I. Latar Belakang

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, pembatasan akses sangat penting diperlukan dalam mengamankan sebuah informasi atau dengan kata lain dapat di istilahkan dengan private area.

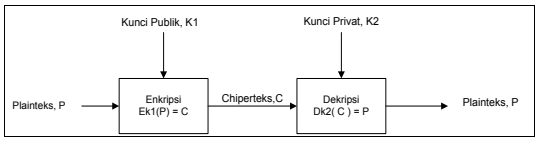
Privasi atau kerahasiaan merupakan bagian yang sangat penting untuk mencegah terbukanya akses terhadap data-data penting atau sensitif oleh orang-orang yang tidak berhak (anonymous). Salah satu cara yang dapat digunakan dalam mengamankan data yaitu menggunakan pendekatan kriptografi. Beberapa cara yang dapat dilakukan untuk mencegah pencurian data yaitu dengan cara mengamankan data dengan pendekatan kriptografi pada sebuah system. Algoritma enkripsi yang sering digunakan, salah satunya adalah RSA (Rivest-Shamir-Adleman).

Pada kasus digital signature penggunaan RSA sangat cocok diimplementasikan [1], dan RSA juga menjadi salah satu teknik enkripsi yang paling maju dalam bidang kriptografi public key [2]. Beberapa penelitian RSA dilakukan diantaranya menggunakan kombinasi algoritma Caesar cipher dan RSA untuk pengamanan dokumen dan menghasilkan kesimpulan bahwa keaslian data lebih terjamin dengan menggunakan RSA [3], mengaplikasikan penggunaan RSA pada sistem penjualan yang

akan dibangun, hasilnya data dalam database khususnya terkait angka penjualan tidak dimengerti oleh pihak yang tidak berkepentingan [4].

II. Kajian Literatur

Salah satu algoritma yang menerapkan konsep kriptografi kunci publik (public key cryptography) yaitu algoritma RSA. Penggunaan algoritma RSA banyak digunakan dan salah saat ini menjadi yang paling termutakhir 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 [5]

Proses generate key pada metode algoritma Kriptografi RSA menggunakan beberapa persamaan, 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 × q
c. Totient(n) = (p - 1) (q – 1)
d. e (Kunci Enkripsi)
e. d (Kunci Deskripsi)
f. m (Plaintext)
g. c (Ciphertext)

Rumus pembuatan algoritma RSA berdasarkan pada persamaan matematika dan teorema Euler sehingga mendapatkan rumus untuk enkripsi [5]. 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

III. Metodologi

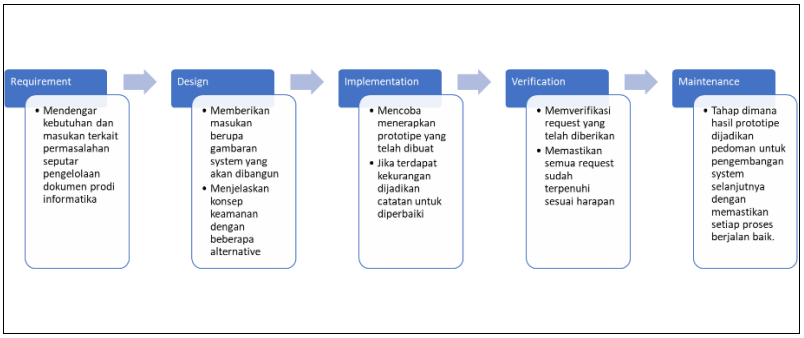
Metode penelitian yang dilakukan berdasarkan hasil wawancara dan data terkait jenis dokumen yang dianggap penting. Observasi pada objek penelitian untuk mendapatkan data primer yang digunakan dalam mengembangkan keamanan dengan RSA untuk menguji keamanan dokumen. Pengembangan sistem algoritma RSA terlihat pada gambar 1 [5].

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, metode waterfall (air terjun) memastikan bahwa langkah logis pada setiap proses harus dilakukan sepanjang siklus pengembangan software (SDLC) yang terdiri dari beberapa tahapan penelitian [6].

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 [9].

6. Operation & Maintenance (Pemeliharaan)
   Tahap untuk melakukan pemeliharaan untuk menjaga sistem tetap berjalan sebagai mana yang diharapkan [10].

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.

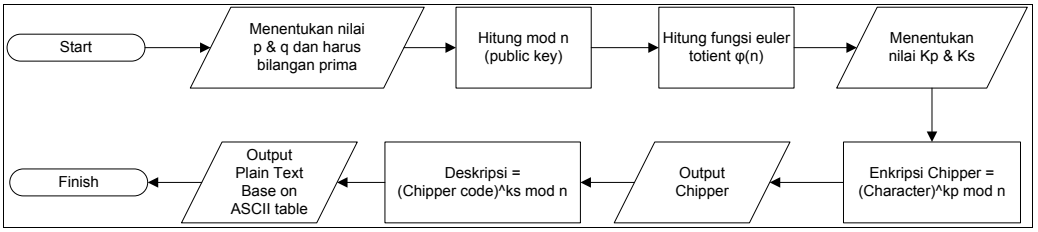


Gambar 2. Proses waterfall sistem keamanan dokumen [10]

IV. Pembahasan

A. Proses RSA

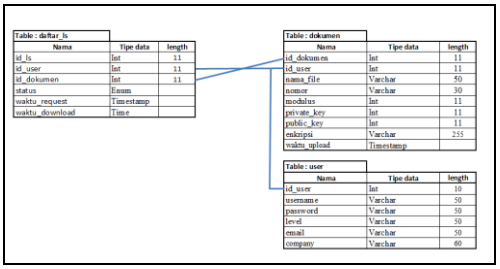
Skema arsitektur dalam penerapan keamanan RSA dimulai dari tahap menentukan nilai, menghitung mod n untuk digunakan sebegai public key, menghitung fungsi euler, hingga tahap akhir mendapatkan kode chipper code. Detail proses RSA seperti pada gambar 3.



Gambar 3. Proses RSA

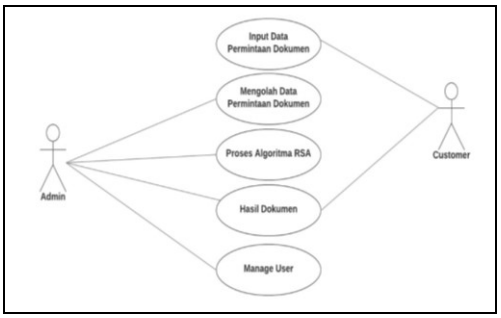
B. Sistem dan design software

Keterwakilan sebuah dekomposisi domain subjek menjadi entitas pada penelitian ini menggunakan pendekatan Entity Relational Diagram (ERD). ERD merupakan node yang mewakili tipe entitas, dan edge (garis asosiasi) yang menggambarkan hubungan dari setiap entitas [8], Hasil pembuatan ERD diperlihatkan pada Gambar 4



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 pada gambar 5.

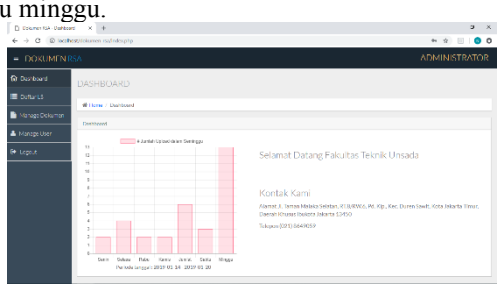


Gambar 5. Use Case Diagram

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.

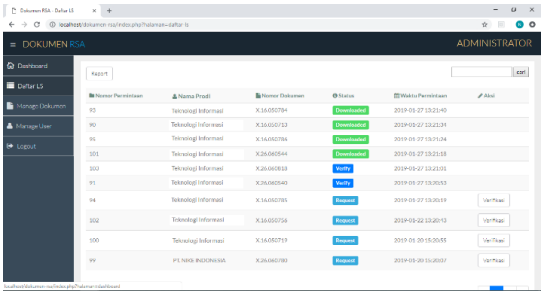
C. Implementaasi

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.



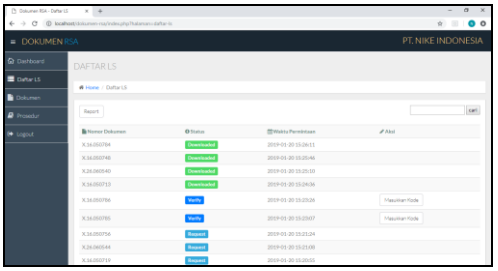
Gambar 6. Halaman Dashboard

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.



Gambar 7. Halaman permintaan dokumen

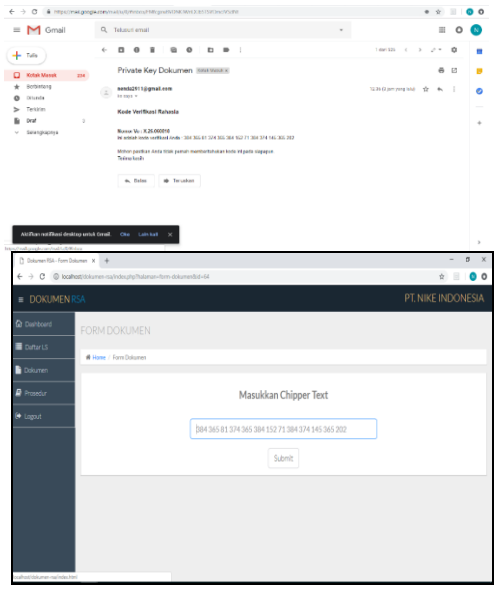
Jika informasi pada status berisi request berarti ada permintaan dokumen dari user dimana terdapat tombol verifikasi yang jika di klik oleh admin maka status akan berubah menjadi verify dan tombol verifikasi akan otomatis hilang. Jika informasi status berisi downloaded berarti user telah berhasil mendownload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

Informasi : KS -Kurang Sekali, K - Kurang, C - Cukup, B - Baik, BS - Baik Sekali

TABLE III
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%	10%

Informasi : KS -Kurang Sekali, K - Kurang, C - Cukup, B - Baik, BS - Baik Sekali

V. Kesimpulan

Kesimpulan penelitian yang didapatkan dari 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%.

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

Ucapan Terima Kasih

Terima kasih kepada LP2MK Universitas Darma Persada, dan tim CBIS Journal Putera Batam atas kerja sama dan koordinasi yang baik sehingga terbitnya jurnal ini.

Daftar Pustaka

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

[9] T. Tukino, "Perancangan Sistem Informasi Pelaporan Gangguan Dan Restitusi Pelanggan Internet Corporate Berbasis Web (Studi Kasus Di PT. Indosat Mega Media West Regional)," *J. Ilm. Inform.*, vol. 6, no. 01, p. 1, 2018, doi: 10.33884/jif.v6i01.324.

[10] Tukino and Amrizal, "Perancangan Sistem Informasi Pelaporan Transaksi Berbasis Web Pada PT Pos Indonesia Batam," *Teknosi*, vol. 03, no. 01, pp. 199–210, 2017.