**LAPORAN PRAKTIKUM**

**PRAKTIK SISTEM KEAMANAN DATA**

**“RESUME JURNAL ALGORITMA RSA(RIVEST SHAMIR ADLEMAN)”**

Dosen Pengampu : Yusuf Fadlila Rachman, S.Kom., M. Kom.



Disusun oleh :

Muhammad Hanif Arafi V3920038

Narutama Phinda Baskara V3920042

Oktarinia Rossa Atanaswati V3920046

Wibiati Sekar Kinasih V3920061

**PROGRAM STUDI DIII TEKNIK INFORMATIKA PSDKU**

**SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**2021**

**RESUME JURNAL 1 (Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP)**

a. Judul dan Latar Belakang Masalah

Judul yang diangkat dalam jurnal ini adalah “*Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP”*, latar belakang yang diangkat dalam jurnal ini adalah karena seiring pesatnya perkembangan teknologi membuat sebuah data menjadi suatu hal yang penting untuk diamankan karena jika tidak privasi akan suatu individu menjadi terganggu dan mungkin bisa disalah gunakan oleh kelompok tertentu,Oleh karenanya, salah satu cara untuk mengamankannya dengan menggunakan metode kriptografi yang mengusung RSA ini, yang merupakan jenis kriptografi asimetris 2 kunci yaitu public dan private.

b. Tujuan Penelitian

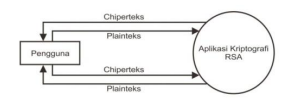
Tujuan dari penelitian ini adalah untuk mengetahui bagaimana cara meningkatkan keamanan suatu data menggunakan metode kriptografi RSA pada suatu file teks berbasis PHP.

c. Algoritma yang dipakai beserta alur penelitiannya

Algoritma yang digunakan pada jurnal ini adalah algoritma RSA. Sementara itu, alur penelitian pada jurnal tersebut adalah sebagai berikut:

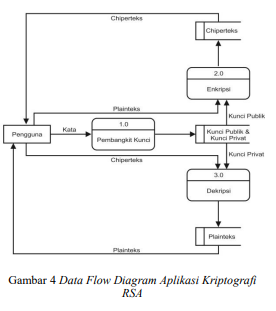
1. Diagram konteks

Diagram konteks merupakan diagram alir tingkat tinggi yang menggambarkan seluruh jaringan, masukan, dan keluaran.



1. Data Flow Diagram

*Data Flow Diagram* (DFD) digunakan untuk menggambarkan suatu sistem yang sedang berjalan. Berikut adalah rancangan DFD pada jurnal tersebut.

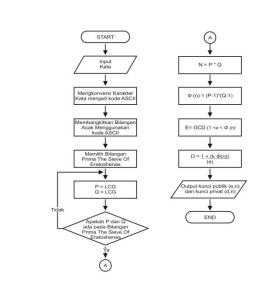


1. Rancangan Flowchart Pembangkitan Kunci

Algoritma RSA melibatkan 2 kunci, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Kunci untuk algoritma RSA dihasilkan dengan cara berikut:

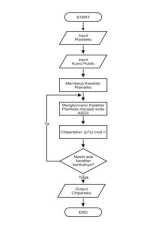
* Pilih dua bilangan prima p dan q secara acak.
* Hitung n = p \* q.
* Pilih bilangan e secara acak di mana e tidak memiliki faktor pembagi yang sama dengan (p1)(q-1) selain bilangan 1.
* Hitung d sedemikian sehingga ed= 1 (mod Φ(n)). Dengan menggunakan sebuah algoritma yang disebut algoritma Euclid akan menghitung d sehingga, d= (1 + k Φ(n))/e.
* Bilangan n dan e kita sebarkan ke publik. e ini adalah yang akan menjadi kunci publik. d menjadi kunci privat.

Kunci publik terdiri dari modulus n dan e (atau enkripsi) eksponen publik. Kunci privat terdiri dari modulus n dan (atau dekripsi) eksponen d yang harus dirahasiakan.



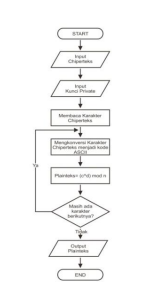
1. Rancangan Flowchart Enkripsi

Data yang diinputkan diubah ke dalam bentuk ASCII, kemudian plaintext dinyatakan ke dalam blok-blok. Blok-blok tersebut selanjutnya dienkripsi dengan metode exponentiation yaitu dengan rumus C = (P)e mod n.



1. Rancangan Flowchart Dekripsi

Ciphertext didekripsi dengan metode exponentiation yaitu dengan rumus P = (C)d mod n. Kemudian hasilnya diubah menjadi karakter ASCII.



1. Rancangan Interface Pembangkit Kunci

Rancangan interface ini adalah form utama pada saat aplikasi pertama kali dijalankan.



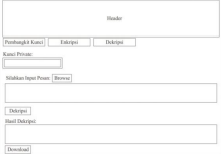
1. Rancangan Interface Enkripsi

Rancangan interface ini adalah form yang digunakan untuk enkripsi plainteks menjadi cipherteks.



1. Rancangan Interface Dekripsi

Rancangan interface ini adalah form yang digunakan untuk dekripsi cipherteks menjadi plainteks.



1. Tampilan Interface Pembangkit Kunci



1. Tampilan Interface Enkripsi



1. Tampilan Interface Dekripsi



d. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Pada penelitian jurnal tersebut dalam proses mengamankan suatu file teks berbasis PHP dengan menggunakan metode RSA, dimulai dari tahapan diagram konteks, data flow diagram, flowchart pembangkitan kunci, flowchart enkripsi, dan lainnya. Adapun kesimpulan dari penelitian ini diantaranya :

* Kombinasi Algoritma LCG sebagai pembangkit bilangan acak dan algoritma The Sieve of Eratosthenes sebagai pembangkit bilangan prima dapat digunakan sebagai pembangkit public dan private pada perancangan kriptografi RSA
* Kunci public dan private hanya dapat dibangkitkan apabila bilangan acak yang dibangkitkan dengan LCG (Linear Congruential Code for Information) menghasilkan lebih dari satu bilangan prima.
* Dikarenakan Chiperteks merupakan hasil dari kombinasi plainteks dan kunci maka file Chiperteks yang merupakan hasil enkripsi memiliki kapasitas lebih besar dibandingkan file plainteks.

e. Kelebihan dan kekurangan jurnal

1. Kelebihan

* Penjelasan di Pendahuluan lumayan jelas dan detail sehingga pembaca mengetahui isi dengan baik
* penjelasan Algoritma RSA lumayan detail sehingga pembaca mengetahui dasar dasarannya
* Konsep Pada Pembuatan Enkripsi lumayan jelas

1. Kekurangan

* Struktur yang membingungkan
* Pada Algoritma Kriptografi RSA di bagian dua bilangan prima p dan q tidak di jelaskan secara detail

**RESUME JURNAL 2 (Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam)**

a. Judul dan Latar Belakang Masalah

Jurnal yang digunakan berjudul “Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam”. Latar belakang masalah pada jurnal tersebut adalah keamanan data yang penting dilakukan untuk melindungi dan menjaga kerahasiaan data informasi anggota koperasi kredit. Dengan demikian, diperlukan teknik pengaman tambahan untuk menjaga keamanan data tersebut sehingga data akan tetap terjaga kerahasiaannya dari orang-orang yang tidak berhak. Salah satu teknik untuk meningkatkan keamanan data adalah dengan menggunakan algoritma kriptografi di mana di dalamnya terdapat proses enkripsi dan dekripsi. Dengan melakukan enkripsi pada suatu data, maka data tersebut tidak dapat terbaca karena teks asli atau plaintext telah diubah ke teks yang tak terbaca atau disebut chipertext. Salah satu algoritma tersebut adalah algoritma RSA yang merupakan jenis kriptografi asimetris yang memakai sepasang kunci publik dan kunci rahasia.

b. Tujuan Penelitian

Tujuan Penelitian untuk mengimplementasi pengamanan data Simpan Pinjam dengan menggunakan teknik Kriptografi dengan Algoritma RSA dan dapat memperlajari Proses Pembuatan Kunci.

c. Algoritma yang dipakai beserta alur penelitiannya

Algoritma yang digunakan pada jurnal ini adalah algoritma RSA. Pada proses enkripsi menggunakan kunci public, sedangkan pada proses dekripsi menggunakan kunci private.

* **Proses Pembangkit Kunci**

Pembangkit kunci merupakan bilangan yang menentukan kunci enkripsi (public key) dan kunci dekripsi (private key) dengan syarat itu yaitu :

1. Pilih bilangan prima sembarang untuk nilai p(prima) dan q (quotient). Pada penelitian dalam jurnal nilai p adalah 47 dan nilai q adalah 71.
2. untuk mencari nilai dari kedua bilangan prima, perlu dilakukan perkalian antara p dan q sehingga n = p \* q = 47 \* 71 = 3337.
3. Hitung m = (p – 1)(q – 1) = 46 \* 70 = 3220.
4. Pilih nilai e dengan syarat e > 1 dan greatest common divisior (e,3220) = 1 nilai e yang diambil adalah 101.

Bukti : (101,3220)

3220 mod 101=89

101 mod 89 = 12

89 mod 12 = 5

12 mod 5 = 2

5 mod 2 = 1

2 mod 1=0

1. Sehingga d e = 1 (mod 3220) dan d < 3220

Mencari nilai = d x 101 = 1 mod 3220

d x 101 mod 3220 = 1

d = 1881

Bukti : 1881 x 101 mod 3220 = 1

Sehingga pasangan kunci yang didapat adalah kunci enkripsi (public key) =(101,3337) dan kunci dekripsi (private key) = (1881,3337).

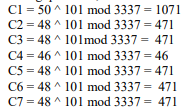
* **Proses Enkripsi**

Setelah didapat perhitungan diatas, maka akan dilakukan enkripsi plaintext P = 200000. Langkah-langkah enkripsi adalah sebagai berikut:

1. mengubah plaintext ke dalam format ASCII.



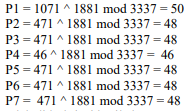
1. Menyatakan plaintext ke dalam blok-blok sehingga setiap blok merepresentasikan nilai di dalam selang [0, n-1].
2. Setiap blok plaintext akan dihitung menggunakan rumus Ci = (Pi)e mod n. Berikut ini merupakan hasil perhitungan antara blok-blok palintext dengan rumus.



1. Dengan demikian ciphertext yang didapatkan C = 1071 471 471 46 471 471 471.

* **Proses Dekripsi**

1. Setelah chipertext dari 200.000 didapat, untuk mengubah kembali jadi plaintext menggunakan dekripsi dengan rumus Pi = (Ci )d mod n. Berikut ini adalah perhitungan dan hasilnya.



1. Setelah berhasil didekripsi hasilnya adalah 50 48 48 46 48 48 48.
2. Mengubah hasil dekripsi tersebut dalam karakter ASCII. Maka hasil dekripsinya adalah plaintext.



d. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Dari hasil pembahasan pada bab sebelumnya dan pengamatan yang telah dilakukan maka dapat diambil kesimpulan diantaranya sebagai berikut:

1. Memecahkan permasalahan yang terjadi berkenaan dengan pengamanan data Simpan Pinjam yaitu menggunakan teknik Kriptografi dengan Algoritma RSA.
2. Untuk merancang Aplikasi Algoritma RSA melalui 3 tahap yang pertama kita harus membangkitkan kunci dengan menggunakan bilangan prima, proses Enkripsi, lalu proses Dekripsi
3. Dengan cara menginstal aplikasi Visual Basic 2010 dan menerapkan pengkodean untuk sistem pengamanan yang sudah ditentukan untuk teknik kriptografi dan algoritma RSA
4. Untuk menguji sistem yang dirancang dilihat dari kualitas perangkat lunak dan mempresentasikan kajian pokok dan spesifikasi, desain dan pengkodean dalam menjalankan sebuah program seperti pengujian sistem yang telah dirancang berjalan sesuai dengan yang diharapkan
5. Implementasi sistem keamanan data menggunakan 2 buah kunci dan prosesnya sedikit lama, karena harus memfaktorkan bilangan prima untuk mendapatkan dua buah kunci agar tidak mudah dipecah oleh pihak lain yang tidak berkepentingan bagi para anggota di CU Suka Makmur

e. Kelebihan dan kekurangan jurnal

Kelebihan :

- Isi jurnal singkat dan jelas dan berbobot

- Proses enkripsi dan dekripsinya mudah dipahami

- Proses pembahasannya langsung diterapkan dalam studi kasus

Kekurangan :

- Kurangnya landasan teori mengenai algoritma RSA itu sendiri

- Tidak dilengkapi dengan tabel ASCII pada bagian pembahasannya

- Abstract dan Pendahuluan, konteks pembahasan yang cenderung sama