REVIEW JURNAL
PENELITIAN DALAM BIDANG ILMU KOMPUTER

Ditujukan untuk memenuhi salah satu tugas mata kuliah Metode Penelitian yang diampu oleh Ibu Riani Lubis, S.T., M.T.

disusun oleh :

10114243 - Fajar Fauzi Ramadhan
10113463 - Muhammad Heda N
10113026 - Bintang Januari Haliri
10113320 - Rizky Wijayamulya

KELOMPOK 6
METODE PENELITIAN – 2

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS KOMPUTER INDONESIA

2016

TABEL REVIEW JURNAL NASIONAL

JUDUL	Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris
JURNAL	Jurnal Komputer dan Informatika (KOMPUTA)
VOLUME & HALAMAN	Vol. 1

TAHUN	2012
PENULIS	**Munawar** *Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer* *Universitas Komputer Indonesia* *Jl. Dipati Ukur No. 112-116 Bandung* munawarhfz@gmail.com
REVIEWER	10114243 – Fajar Fauzi Ramadhan 10113463 – Muhammad Heda N 10113026 – Bintang J. Haliri 10113320 – Rizky Wijayamulya
TANGGAL	24 Oktober 2016

TUJUAN PENELITIAN	Makalah ini bertujuan untuk memunculkan kepedulian bagi para perancang sistem informasi terhadap keamanan data bahwa keamanan data merupakan bagian utama sistem yang patut untuk di perhitungkan, memunculkan ide atau metode baru bagi para perancang sistem informasi dalam mengamankan data atau informasi yang di kelolahnya, memberikan warna baru dalam ilmu penyandian data atau cryptography.
SUBJEK PENELITIAN	Perusahaan dibidang keuangan, Pemerintahan, Perkantoran, Organisasi dan Individu.
METODE PENELITIAN	Metode kualitatif karena peneliti mengembangkan kualitas yang baru untuk menghasilkan algoritma kriptografi yang baru.
LANGKAH-LANGKAH PERANCANGAN 1. 2. 3. 4. 5.	Langkah-langkah yang digunakan dalam proses penelitian ini adalah: 1. Menjelaskan tentang **Enkripsi dan Dekripsi** 2. Mengetahui tentang **Penggolongan Cryptographic system (cryptosystem).** 3. Menjelaskan tentang **Pemrosesan kunci private, public, enkripsi data 2048 bit** 4. Pengujian Program dengan file dokumen, gambar, audio dan video.
HASIL PENELITIAN	Berdasarkan hasil analisa, perancangan, implementasi dan pengujian program, maka dapat diambil beberapa kesimpulan diantaranya: 1. Algoritma kriptografi ini dibuat dan dirancang sendiri oleh penulis untuk dapat diterapkan pada program aplikasi, sehingga memiliki kelebihan dalam pengamanan data atau informasi. Hal ini dikarenakan data hasil enkripsi sangat sulit untuk dimengerti dan diterjemahkan, karena banyaknya operasi logika yang harus dilewati serta algoritma yang

	dibuat masih belum terpublikasi secara umum. 2. Kerahasiaan kunci lebih terjaga karena menggunakan konsep kriptografi asimetris, memiliki kunci private dan kunci publik yang memiliki fungsi yang berbeda dan juga didukung oleh panjang kunci private yang relatif lebih panjang yaitu 1024 bit 3. Algoritma yang dibuat mengunakan kombinasi kunci yang sulit terprediksi, dikarenakan dalam membuat kunci private dan kunci publik menggunakan kombinasi kunci sesi yang diinputkan user, waktu dan tanggal input serta ID processor. Sehingga pada waktu akses serta pada komputer yang berbeda dapat menghasilkan kunci yang berbeda pula meskipun dengan inputan kunci sesi yang sama. 4. Program dibuat sesederhana mungkin, sehingga user bisa dengan mudah mengenali setiap fungsi dari tombol-tombol yang digunakan dalam aplikasi ini. 5. Program kriptografi ini bisa digunakan untuk melakukan enkripsi semua file misalnya gambar, dokumen, audio maupun video dan juga jenis file yang lain. 6. Program yang dibuat dapat diimplementasikan pada sebuah jaringan (LAN). Sehingga program ini bisa dipakai untuk melindungi data, baik yang ada dikomputer server maupun di komputer client.

TABEL REVIEW JURNAL INTERNASIONAL

JUDUL	Cryptographic Algorithms for Secure Data Communication
JURNAL	International Journal of Computer Science and Security
VOLUME & HALAMAN	Vol. 5 Hal.17
TAHUN	2011
PENULIS	**Zirra Peter Buba** zirrapeter@yahoo.com *Department of Mathematical Sciences* *Adamawa State University* *Mubi, 650221, Nigeria.* **Gregory Maksha Wajiga** gwajiga@gmail.com *Department of Mathematics and Computer Science* *Federal University of Technology* *Yola, 640284, Nigeria.*
REVIEWER	10114243 – Fajar Fauzi Ramadhan 10113463 – Muhammad Heda N

	10113026 – Bintang J. Haliri 10113320 – Rizky Wijayamulya
TANGGAL	24 Oktober 2016

TUJUAN PENELITIAN	Makalah ini bertujuan untuk menyajikan algoritma kriptografi baru untuk sarana komunikasi melalui saluran aman dan memastikan bahwa penyusup tidak memiliki akses ke plaintext tanpa kunci rahasia. Algoritma yang ini memunculkan pesan enkripsi kedalam persamaan non-linear dengan menggunakan kunci publik dan menguraikan partai yang dimaksud menggunakan kunci pribadi.
SUBJEK PENELITIAN	Perkantoran, Organisasi dan Individu.
METODE PENELITIAN	Metode kualitatif karena peneliti mengembangkan kualitas yang baru untuk menghasilkan algoritma kriptografi yang baru.
LANGKAH-LANGKAH PERANCANGAN 6. 7. 8. 9. 10. 11. 12. 13. 14.	Langkah-langkah yang digunakan dalam proses penelitian ini adalah: 1. Menjelaskan tentang **Modern Key-Based Cryptographic Techniques** 2. Mengetahui tentang **Types of Attacks** 3. Menjelaskan tentang **Types of Encryption Algorithms** 4. Menerapkan usulan algoritma enkripsi melalui 3 tahanpan - Melalui Flowchart - Mengubah kata-kata kompresi ke dalam sistem persamaan non linier. C. Menerapkan prinsip-prinsip delta () encoding 5. Pengujian usulan algoritma enkripsi melalui proses enkripsi dan dekripsi sehingga mendapatkan result yang terbukti dari algoritma yang diusulkan.
HASIL PENELITIAN	Menunjukan bagaimana orang dapat mengamankan informasi penting dan sensitive yang disimpan atau dikirimkan melalui saluran komunkasi yang menggunakan kunci enkripsi dan dekripsi yang kuat dan algoritma yang usulkan telah terbukti untuk menahan setiap jenis serangan tetapi kekuatan sebuah skema enkripsi adalah bergantung pada kerahasiaan kunci.

TABEL PERBANDINGAN HASIL REVIEW JURNAL INTERNASIONAL DAN NASIONAL

Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris
dan
Cryptographic Algorithms For Secure Data Communication

TABEL PERSAMAAN

JURNAL	NASIONAL	INTERNASIONAL
PEMBAHASAN	Sistem keamanan menggunakan metode kriptografi	Sistem keamanan menggunakan metode kriptografi
METODE	Kualitatif	Kualitatif
OBJEK PENELITIAN	Data File	Data File
SUBJEK PENELITIAN	Perkantoran, Organisasi dan Individu.	Perkantoran, Organisasi dan Individu.

TABEL PERBEDAAN

JURNAL	NASIONAL	INTERNASIONAL
LANGKAH-LANGKAH	Langkah-langkah yang digunakan dalam proses penelitian ini adalah: 22. 1. Menjelaskan tentang	Langkah-langkah yang digunakan dalam proses penelitian ini adalah: 1. Menjelaskan tentang **Modern Key-Based**

	Enkripsi dan Dekripsi 2. Mengetahui tentang **Penggolongan Cryptographic system (cryptosystem).** 3. Menjelaskan tentang **Pemrosesan kunci private, public, enkripsi data 2048 bit.** 4. Pengujian Program dengan file dokumen, gambar, audio dan video.	**Cryptographic Techniques** 2. Mengetahui tentang **Types of Attacks** 3. Menjelaskan tentang **Types of Encryption Algorithms** 4. Menerapkan usulan algoritma enkripsi melalui 3 tahanpan -Melalui Flowchart -Mengubah kata-kata kompresi ke dalam sistem persamaan non linier. -Menerapkan prinsip-prinsip delta () encoding 5. Pengujian usulan algoritma enkripsi melalui proses enkripsi dan dekripsi sehingga mendapatkan result yang terbukti dari algoritma yang diusulkan.