NAMA : ASYROFI FADHIL AL-AHADI

NIM : 1310651182

1. Carilah tiga buah paper yang membahas tentang IT Security? Kemudian Anda buat review dari paper tersebut. Review yang akan dikerjakan mengacu pada contoh berikut :

No	Peneliti	Judul	Tool	Hasil
1	Nova Bintoro Ekaputra	Aplikasi Kriptografi Untuk Sistem Keamanan Penyimpanan Data atau Informasi Hasil Penelitian yang Bersifat Rahasia	Visual Basic 6.0	Aplikasi ini, menggunakan algoritma MARS dengan modus ECB (Electronic Code Book.MARS sebagai salah satu kandidat AES(Advanced Encrypted Standard), memiliki kelebihan yaitu mempunyai tingkat keamanan dan proses kecepatan yang tinggi.
2	Edhy Suatanta	Aplikasi E-LEARNING di IST AKPRIND YOGYAKARTA	Apache,PHP,PostgreSQL	Web server aplikasi e-Learning IST AKPRIND dibangun menggunakan Apache 2.2.3 dengan sistem operasi Debian, bahasa pemrograman PHP versi 5.2.0, dan database server menggunakan PostgreSQL.
3	Ahmaddul Hadi	Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademik Menggunakan *Digital Signature* dengan Algoritma Kurva Eliptik		

- **Aplikasi Kriptografi Untuk Sistem Keamanan Penyimpanan Data atau Informasi Hasil Penelitian yang Bersifat Rahasia**

ANALISIS APLIKASI KRIPTOGRAFI UNTUK SISTEM KEAMANAN PENYIMPANAN DATA ATAU INFORMASI HASIL-HASIL PENELITIAN YANG BERSIFAT RAHASIA. Salah satu cara yang digunakan untuk pengamanan data dan atau informasi adalah menggunakan sistem kriptografi. Aplikasi ini, menggunakan algoritma MARS dengan modus ECB (Electronic CodeBook). MARS sebagai salah satu kandidat AES(Advanced Encrypted Standard), memiliki kelebihan yaitu mempunyai tingkat keamanan dan proses kecepatan yang tinggi. Hal ini menjadikan algoritma MARS sebagai pilihan terbaik untuk proses enkripsi yang diperlukan oleh dunia informasi menuju abad berikutnya. Algoritma MARS menggunakan kunci 128 bit dan proses enkripsinya terdiri dari 32 ronde. Program ini dirancang dengan menyediakan unit sarana pengiriman file, baik untuk file yang telah dienkripsi maupun jenis file biasa. Hasil pengujian menunjukkan bahwa program ini dapat berjalan sesuai dengan spesifikasi rancangannya.

- **Aplikasi E-LEARNING di IST AKPRIND YOGYAKARTA**

Seringkali masalah keamanan sistem aplikasi terabaikan justru setelah semua peralatan dan infrastruktur pengaman telah terpasang. Bahkan pentingnya pengamanan baru disadari setelah terjadi bencana. Kerugian sebuah institusi/organisasi yang diakibatkan dari sebuah serangan terhadap sistem aplikasi sangatlah besar, tetapi hal ini sangat sukar dideteksi, karena secara umum tidak akan diakui dengan berbagai alasan. Tanpa pengamanan sistem aplikasi yang baik, penerapan teknologi sehebat apapun akan sangat membahayakan institusi/organisasi itu sendiri. Nilai informasi yang begitu penting dan strategis mengakibatkan serangan dan ancaman terhadap sistem aplikasi dan arus informasi semakin meningkat. Kebutuhan keamanan sistem aplikasi timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak di ijinkan hendak mengakses atau mengubah data. Permasalahan lainnya mencakup perlindungan data dari delay yang berlebihan pada saat mengakses atau menggunakan data, atau mengatasi gangguan *Denial of Service* (DoS).

Aplikasi *e-Learning* IST AKPRIND Yogyakarta merupakan program aplikasi baru yang telah dikembangkan, dipublikasikan, dan diterapkan dalam proses pembelajaran, namun belum diuji keamanannya. Penelitian ini dilakukan untuk menganalisis aspek keamanan sistem aplikasi yang meliputi *web server*, program aplikasi, dan *database server* dengan tujuan untuk meningkatkan aspek keamanan pada aplikasi *e-Learning* yang diterapkan.

Berdasarkan hasil penelitian, dapat dinyatakan bahwa tingkat ancaman terhadap web server
dan program aplikasi aplikasi *e-Learning* IST AKPRIND berada pada level 2 (Medium). Hal tersebut menunjukkan bahwa masih terdapat banyak celah yang memungkinkan terjadinya ancaman dan akses ilegal yang berpotensi merusak sistem. Sedangkan *database server* aplikasi *e-Learning* IST AKPRIND aman terhadap kemungkinan adanya ancaman dan akses ilegal yang berpotensi merusak.

- **Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademik Menggunakan *Digital Signature* dengan Algoritma Kurva Eliptik**

Pengamanan dokumen pada setiap lembaran informasi Sistem Informasi Akademik (SIA) UNP dengan menambahkan tanda tangan digital. Penggunaan tanda tangan digital (*Digital Signature*) kurva eliptik didasarkan atas *Elliptic Curve Discrete Logarithm Problem* (ECDLP) pada kurva eliptik modulo prima memiliki tingkat keamanan yang tinggi.
Aplikasi SIA pada penelitian ini menghasilkan output dokumen tercetak yang telah ditambahkan (*embedded*) dengan tanda tangan. Tanda tangan berupa Informasi (*plaintext*) yang di-enkripsi pada proses *signing* yaitu NIM, IP, jenis dokumen dan waktu cetak dimana ke empat variabel ini di-enkripsi dengan algoritma kurva eliptik pada bidang terbatas F

dan menghasilkan kunci *public r* yang tersimpan pada sebuah tabel database, kunci *private s* serta *chipertext* (*ds code*). Pada aplikasi pengujian tandatangan (*verifying*) dengan mendekripsikan *chipertext (ds code)* yang diinputkan, jika nilai kunci publik dan ke empat variabel cocok maka ditampilkan informasi valid dari dokumen. Pengujian tingkat keamanan dan kehandalan tanda tangan dengan menggunakan program *sniffing wireshark* dan *chain & abel.* Dan pengujian kinerja laman web dengan menggunakan aplikasi *firebug*.
Penelitian tesis ini menghasilkan aplikasi SIA yang telah ditambahkan tanda tangan dan aplikasi pembaca keabsahan tanda tangan. Dari hasil uji coba tanda tangan tidak dapat dihacking dan dicracking dengan aplikasi pengendus, serta aplikasi *perifying* menunjukkan waktu akses rata-rata 110 ms. Aplikasi web *verifying* membutuhkan waktu yang lama untuk mendekripsikan digital signature, tetapi ini sebanding dengan keamanan dan kehandalan yang dihasilkan oleh sistim informasi dengan algoritma kurva eliptik ini.

2. Berikut ini ada file ciphertext misterius

   VGlkYWsgc2VnYW1wYW5nIGl0dWxhaCBtYXMgYnJvLiBkZWNyeXB0IGluaTogDQo2ODc0NzQ3MDNhMmYyZjY0NmMyZTY0NzI2ZjcwNjI2Zjc4MmU2MzZmNmQyZjczMmYzMjM0NjkzMTZiNzEzNjc5NjM2ZjZmNjg3MTZhNmMyZjYzNzI3OTcwNzQ2ZjMxNDY2YzYxNjcyZTZkNzAzMw==

   Anda sebagai seorang ahli forensik diminta untuk menyelidiki maksud yang tersembunyi pada cipher tersebut. Berikan analisis Anda dan tuliskan langkah-langkah untuk menemukan "sesuatu" yang tersembunyi pada cipher tersebut.

A. Pertama kita download sebuah tool yang bernama Forensic Toolkit
B. Lalu kita instal aplikasi tersebut sampai finish.
C. Lalu pilih New Case, kemudian akan muncul :

- investigator name = isi sesuai keinginan
- Case Number = isi sesuai keinginan

- Case Name= isi sesuai keinginan
- Case path= isi sesuai keinginan
- Case folder= isi sesuai keinginan

D. Next > forensic examiner information
E. Next > proseses to perform, next sampai dengan add evidence
F. Klik add evidence continue lalu kita ambil file audio tersebut .
G. OK dan kita buka di penyimpanan awal yang klita lakukan > kita bisa melihat atau memutar audio tersebut.