

**UTS**  
**KEAMANAN INFORMASI**



**NAMA : RAHMAT HIKMATULLAH**

**NIM : 1310652047**

**TEKNIK INFORMATIKA**  
**UNIVERSITAS MUHAMMADIYAH JEMBER**

## ANTISIPASI CYBERCRIME MENGGUNAKAN TEKNIK KOMPUTER FORENSIK

**Yudi Prayudi, Dedy Setyo Afrianto**

*Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia*

*Jl. Kaliurang Km. 14 Yogyakarta 55501*

*Telp. (0274) 895287 ext. 122, Faks. (0274) 895007 ext. 148*

*e-mail: prayudi@fti.uui.ac.id*

### ABSTRAKSI

Perkembangan pesat dari teknologi informasi ternyata juga diikuti oleh berkembangnya isu seputar keamanan dan kejahatan komputer. Berbagai modus kejahatan baru berbantuan komputer mulai banyak dirasakan oleh masyarakat. Selain perangkat hukum dalam bentuk aturan dan undang-undang, maka dari aspek ilmiah dan teknis juga diperlukan mekanisme pembuktian kejahatan tersebut. Dalam hal ini komputer forensik adalah satu bidang yang akan sangat mendukung upaya-upaya penegakan hukum terhadap tindak kejahatan berbantuan komputer. Makalah ini memberikan gambaran singkat terkait pengertian, metode dan implementasi proses forensik menggunakan sejumlah aplikasi yang tersedia.

**Kata kunci:** cybercrime, forensik, investigasi, bukti digital.

### 1. PENDAHULUAN

Perkembangan Teknologi Informasi dan Komputer (TIK) telah mengalami kemajuan yang sangat pesat, terutama sekali setelah diketemukannya teknologi yang menghubungkan antar komputer (*Networking*) dan Internet. Namun demikian, berbagai kemajuan tersebut ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan. Istilah ini kemudian dikenal dengan *cybercrime*.

Permasalahan yang diakibatkan oleh penggunaan komputer untuk kepentingan diatas telah mulai menimbulkan berbagai dampak negatif. Baik secara mikro yang dampaknya hanya pada tingkatan personal/perseorangan, maupun secara makro yang berdampak pada wilayah komunal, publik, serta memiliki efek domino yang luas. Untuk menangani permasalahan ini, maka di beberapa negara telah dibentuk unit khusus kepolisian yang berfungsi sebagai penindak kejahatan yang spesifik terkait dengan permasalahan *cybercrime*.

#### 1.1 Kasus Cybercrime

Berbagai permasalahan yang muncul terkait dengan *cybercrime* telah menyedot perhatian berbagai kalangan yang berhubungan dengan bidang TIK. Hal ini dipicu oleh semakin luasnya dimensi kejahatan di bidang cybercrime ini. Contoh kasusnya antara lain adalah:

- a. Menurut *Internet Fraud Complaint Center* (IFCC), mitra dari *Federal Bureau and Investigation* (FBI) dan *National White Collar Crime Center*, antara Mei 2000 dan Mei 2001, dalam operasi tahun pertama, website IFCC menerima 30.503 keluhan penipuan internet. Laporan lengkap dapat download pada alamat:

[www1.ifccfbi.gov/strategy/IFCC\\_Annual\\_Report.pdf](http://www1.ifccfbi.gov/strategy/IFCC_Annual_Report.pdf).

- b. Menurut Survey Institute Keamanan Komputer pada 2001, bersama dengan Squad Gangguan Komputer dari FBI, 186 responden dari agen perusahaan dan pemerintah melaporkan total kehilangan keuangan diatas US\$3.5 juta, sebagian besar terjadi karena pencurian informasi kepemilikan dan penipuan keuangan (lihat [www.gocsi.com/press/20020407.html](http://www.gocsi.com/press/20020407.html)).
- c. Menurut *Cybersnitch Voluntary Online Crime* melaporkan sistem kejahatan relasi-internet telah mencakup berbagai aspek mulai dari pemalsuan desktop hingga ke pornografi anak dan juga meliputi kejahatan seperti pencurian elektronik hingga ancaman teroris. (daftar dilaporkan cybercrimes tersedia pada alamat: ([www.cybersnitch.net/csinfo/csdatabase.asp](http://www.cybersnitch.net/csinfo/csdatabase.asp)).)

#### 1.2 Alasan kemunculan Cybercrime

Pada tahun 2002 diperkirakan terdapat sekitar 544 juta orang terkoneksi secara online. Meningkatnya populasi orang yang terkoneksi dengan internet akan menjadi peluang bagi munculnya kejahatan komputer dengan beragam variasi kejahatannya. Dalam hal ini terdapat sejumlah tendensi dari munculnya berbagai gejala kejahatan komputer, antara lain:

- a. Permasalahan finansial. *Cybercrime* adalah alternatif baru untuk mendapatkan uang. Perilaku semacam *carding* (pengambil alihan hak atas kartu kredit tanpa seijin pihak yang sebenarnya mempunyai otoritas), pengalihan rekening telepon dan fasilitas lainnya, ataupun perusahaan dalam bidang tertentu yang mempunyai kepentingan untuk menjatuhkan kompetitornya dalam perebutan *market*, adalah sebagian bentuk cybercrime dengan tendensi finansial.

- b. Adanya permasalahan terkait dengan persoalan politik, militer dan sentimen *Nasionalisme*. Salah satu contoh adalah adanya serangan hacker pada awal tahun 1990, terhadap pesawat pembom paling rahasia Amerika yaitu *Stealth Bomber*. Teknologi tingkat tinggi yang terpasang pada pesawat tersebut telah menjadi lahan yang menarik untuk dijadikan ajang kompetisi antar negara dalam mengembangkan peralatan tempurnya.
- c. Faktor kepuasan pelaku, dalam hal ini terdapat permasalahan psikologis dari pelakunya. Terdapat kecenderungan bahwasanya seseorang dengan kemampuan yang tinggi dalam bidang penyusupan keamanan akan selalu tertantang untuk menerobos berbagai sistem keamanan yang ketat. Kepuasan batin lebih menjadi orientasi utama dibandingkan dengan tujuan finansial ataupun sifat sentimen.

Elemen penting dalam penyelesaian masalah keamanan dan kejahatan dunia komputer adalah penggunaan sains dan teknologi itu sendiri. Dalam hal ini sains dan teknologi dapat digunakan oleh pihak berwenang seperti: penyidik, kepolisian, dan kejaksaan untuk mengidentifikasi tersangka pelaku tindak kriminal.

## 2. KOMPUTER FORENSIK

Forensik adalah proses penggunaan pengetahuan ilmiah dalam mengumpulkan, menganalisa, dan mempresentasikan barang bukti ke pengadilan. Forensik secara inti berhubungan dengan penyelamatan dan analisis barang bukti laten. Barang bukti laten dapat berbentuk dalam banyak format, mulai dari sidik jari di jendela, DNA yang diperoleh dari noda darah sampai file-file di dalam hard disk komputer.

### 2.1 Sejarah Komputer Forensik.

Barang bukti yang berasal dari komputer telah muncul dalam persidangan hampir 30 tahun. Awalnya, hakim menerima bukti tersebut tanpa melakukan pembedaan dengan bentuk bukti lainnya. Sesuai dengan kemajuan teknologi komputer, perlakuan serupa dengan bukti tradisional akhirnya menjadi bermasalah. Bukti-bukti komputer mulai masuk kedalam dokumen resmi hukum lewat *US Federal Rules of Evidence* pada tahun 1976. Selanjutnya dengan berbagai perkembangan yang terjadi muncul beberapa dokumen hukum lainnya, antara lain adalah:

- a. The Electronic Communications Privacy Act 1986, berkaitan dengan penyadapan peralatan elektronik.
- b. The Computer Security Act 1987 (Public Law 100-235), berkaitan dengan keamanan sistem komputer pemerintahan.
- c. Economic Espionage Act 1996, berhubungan dengan pencurian rahasia dagang.

Pembuktian dalam dunia maya memiliki karakteristik tersendiri. Dalam hal ini sifat alami dari teknologi komputer memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya. Karena itulah salah satu upaya untuk mengungkap kejahatan komputer adalah lewat pengujian sistem yang berperan sebagai seorang detektif dan bukannya sebagai seorang user. Kejahatan komputer (*cybercrime*) tidak mengenal batas geografis, aktivitas ini bisa dilakukan dari jarak dekat, ataupun dari jarak ribuan kilometer dengan hasil yang serupa. Penjahat biasanya selangkah lebih maju dari penegak hukum, dalam melindungi diri dan menghancurkan barang bukti. Untuk itu tugas ahli komputer forensik untuk menegakkan hukum dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu akan berguna di persidangan.

### 2.2 Definisi Komputer Forensik

Menurut Marcella [4], secara terminologi, Komputer Forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, [pengambilan/penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer. Istilah ini relatif baru dalam bidang komputer dan teknologi, tapi telah muncul diluar *term* teknologi (berhubungan dengan investigasi dan investigasi bukti-bukti intelejen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.

Menurut Budhisantoso[1], komputer forensik belum dikenali sebagai suatu disiplin pengetahuan yang formal. Dalam hal ini definisi komputer forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sedemikian sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum

Seperti umumnya ilmu forensik lain, komputer forensik juga melibatkan penggunaan teknologi yang rumit, perkakas dan prosedur yang harus diikuti untuk menjamin ketelitian dari pemeliharaan bukti dan ketelitian hasil. Prinsip kerja komputer forensik pada dasarnya mirip dengan proses yang terjadi pada kepolisian ketika hendak mengusut bukti tindak kejahatan dengan menelusuri fakta-fakta yang ada. Hanya saja pada komputer forensik proses dan kejadiannya terdapat pada dunia maya. Selain untuk kepentingan pembuktian, penggunaan forensik komputer secara tepat juga dapat membersihkan seseorang yang tidak bersalah dari dakwaan atau sebaliknya membawa seseorang yang terbukti bersalah dihadapan hukum

### 3. METODOLOGI FORENSIK

Menurut Wright[7] penyelidikan sebaiknya dimulai bila sebuah rencana telah terumuskan dengan baik. Maka landasan metodologi akan memetakan konstruksi ilmiah dalam menyelesaikan

sebuah pekerjaan. Demikian juga dalam komputer forensik, metodologi diharapkan akan membantu tercapainya hasil yang dituju. Walaupun tidak ada standard baku, namun terdapat sejumlah tahapan yang sebaiknya dilakukan dalam proses komputer forensik, yaitu: menentukan tujuan, memproses fakta, mengungkapkan bukti digital.

Tujuan diperlukan sebagai pengarah akhir dari sebuah investigasi. Dalam hal ini sebuah tujuan sebaiknya juga dideskripsikan dalam bentuk parameter-parameter kesuksesan dalam meng-*investigasi* kejadian. Dengan adanya parameter tersebut maka akan diketahui kapan hasil dari inverstigasi telah berakhir.

### 3.1 Pengungkapan Bukti Digital

Bukti digital (*Digital Evidence*) merupakan salahsatu perangkat vital dalam mengungkap tindak *cybercrime*. Dengan mendapatkan bukti-bukti yang memadai dalam sebuah tindak kejahatan, sebenarnya telah terungkap separuh kebenaran. Langkah berikutnya adalah menindak-lanjuti bukti-bukti yang ada sesuai dengan tujuan yang ingin dicapai. Bukti Digital yang dimaksud dapat berupa adalah : E-mail, file-file wordprocessors, spreadsheet, sourcecode dari perangkat lunak, Image, web browser, bookmark, cookies, Kalender.

Menurut Kemmish[3], terdapat empat elemen forensic yang menjadi kunci pengungkapan bukti digital. Elemen forensic tersebut adalah: identifikasi bukti digital, penyimpanan bukti digital, analisa bukti digital, presentasi bukti digital.

### 3.2 Identifikasi Bukti Digital

Elemen ini merupakan tahapan paling awal dalam komputer forensik. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan. *Network Administrator* merupakan sosok pertama yang umumnya mengetahui keberadaan *cybercrime* sebelum sebuah kasus *cybercrime* diusut oleh fihak yang berwenang. Ketika fihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemen-elemen vital lainnya, antara lain:

- a. Petugas Keamanan (*Officer/as a First Responder*), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa, mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan.
- b. Penelaah Bukti (*Investigator*), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti.
- c. Tekhnisi Khusus, memiliki kewenangan tugas antara lain : memelihara bukti yang rentan kerusakan dan menyalin *storage* bukti,

mematikan(*shuting down*) sistem yang sedang berjalan, membungkus/memproteksi bukti-bukti, mengangkut bukti dan memproses bukti.

Ketiga elemen vital diatas itulah yang umumnya memiliki *otoritas* penuh dalam penuntasan kasus *cybercrime* yang terjadi.

### 3.3 Penyimpanan Bukti Digital

Barang bukti digital merupakan barang bukti yang rapuh. Tercemarnya barang bukti digital sangatlah mudah terjadi, baik secara tidak sengaja maupun disengaja. Kesalahan kecil pada penanganan barang bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan.

Bentuk, isi, makna dari bukti digital hendaknya disimpan dalam tempat yang *steril*. Hal ini dilakukan untuk benar-benar memastikan tidak ada perubahan-perubahan. Sedikit terjadi perubahan dalam bukti digital, akan merubah hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, mengalami kecelakaan. Langkah pertama untuk menghindarkan dari kondisi-kondisi demikian salah satunya adalah dengan melakukan copy data secara *Bitstream Image* pada tempat yang sudah pasti aman.

*Bitstream image* adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk File yang tersembunyi (*hidden files*), File temporer (*temp file*), File yang terdefragmen (*fragmen file*), dan file yang belum *ter-overwrite*. Dengan kata lain, setiap biner digit demi digit di-copy secara utuh dalam media baru. Teknik pengkopian ini menggunakan teknik komputasi CRC. Teknik ini umumnya diistilahkan dengan *Cloning Disk* atau *Ghosting*.

### 3.4 Analisa Bukti Digital

Barang bukti setelah disimpan, perlu diproses ulang sebelum diserahkan pada pihak yang membutuhkan. Pada proses inilah skema yang diperlukan akan fleksibel sesuai dengan kasus-kasus yang dihadapi. Barang bukti yang telah didapatkan perlu di-*explore* kembali kedalam sejumlah scenario yang berhubungan dengan tindak pengusutan, antara lain: siapa yang telah melakukan, apa yang telah dilakukan (Contoh : penggunaan software apa saja), hasil proses apa yang dihasilkan, waktu melakukan).

Secara umum, tiap-tiap data yang ditemukan dalam sebuah sistem komputer sebenarnya adalah potensi informasi yang belum diolah, sehingga keberadaannya memiliki sifat yang cukup penting. Data yang dimaksud antara lain : Alamat URL yang telah dikunjungi, Pesan e-mail atau kumpulan alamat e-mail yang terdaftar, Program Word processing atau format ekstensi yang dipakai, Dokumen spreadsheet yang dipakai, format gambar yang dipakai apabila ditemukan, Registry

Windows, Log Event viewers dan Log Applications, File print spool.

### 3.5 Presentasi Bukti Digital

Kesimpulan akan didapatkan ketika semua tahapan telah dilalui, terlepas dari ukuran *obyektifitas* yang didapatkan, atau standar kebenaran yang diperoleh, minimal bahan-bahan inilah nanti yang akan dijadikan “modal” untuk bukti di pengadilan. Selanjutnya bukti-bukti digital inilah yang akan dipersidangkan, diuji otentifikasi dan dikorelasikan dengan kasus yang ada. Pada tahapan ini semua proses-proses yang telah dilakukan sebelumnya akan diurai kebenarannya serta dibuktikan kepada hakim untuk mengungkap data dan informasi kejadian.

## 4. IMPLEMENTASI PROSES KOMPUTER FORENSIK

Untuk melakukan proses forensik pada sistem komputer maka dapat digunakan sejumlah tools yang akan membantu investigator dalam melakukan pekerjaan forensiknya.

Menurut Budhisantoso[1] secara garis besar tools untuk kepentingan komputer forensik dapat dibedakan secara hardware dan software. Hardware tools forensik memiliki kemampuan yang beragam mulai dari yang sederhana dengan komponen *single-purpose* seperti *write blocker* sampai sistem komputer lengkap dengan kemampuan server seperti F.R.E.D (*Forensic Recovery of Evidence Device*). Sementara Tools software forensik dapat dikelompokkan kedalam dua kelompok yaitu aplikasi berbasis *command line* dan aplikasi berbasis GUI.

Baik dari sisi hardware maupun software, tools untuk komputer forensik diharapkan dapat memenuhi 5 fungsi, yaitu untuk kepentingan akuisisi (*acquisition*), validasi dan diskriminasi (*validation and discrimination*), ekstraksi (*extraction*), rekonstruksi (*reconstruction*) dan pelaporan (*reporting*).

Salah satu software yang dapat digunakan untuk kepentingan identifikasi perolehan bukti digital adalah Spy Anytime PC Spy dari Waresight.Inc ([www.waresight.com](http://www.waresight.com)). Kemampuan dari aplikasi ini antara lain adalah untuk monitoring berbagai aktivitas komputer, seperti: *website logs*, *keystroke logs*, *application logs*, *screenshot logs*, *file/folder logs*.

Untuk kepentingan penyimpanan bukti digital, salah satu teknik yang digunakan adalah Cloning Disk atau Ghosting. Teknik ini adalah teknik copy data secara bitstream image..Salah satu aplikasi yang dapat digunakan untuk kepentingan ini adalah NortonGhost 2003 dari Symantec Inc. ([www.symantec.com](http://www.symantec.com)).

Untuk kepentingan analisa bukti digital, salah satu aplikasi yang dapat digunakan adalah Forensic Tools Kit (FTK) dari Access Data Corp

([www.accesdata.com](http://www.accesdata.com)). FTK sebenarnya adalah aplikasi yang sangat memadai untuk kepentingan implementasi Komputer Forensik. Tidak hanya untuk kepentingan analisa bukti digital saja, juga untuk kepentingan pemrosesan bukti digital serta pembuatan laporan akhir untuk kepentingan presentasi bukti digital.

## 5. PENUTUP

Mengingat semakin banyak kasus-kasus yang terindikasi sebagai cybercrime, maka selain aspek hukum maka secara teknis juga perlu disiapkan berbagai upaya preventif terhadap penanggulangan kasus cybercrime. Komputer forensik, sebagai sebuah bidang ilmu baru kiranya dapat dijadikan sebagai dukungan dari aspek ilmiah dan teknis dalam penanganan kasus-kasus cybercrime.

Kedepan profesi sebagai investigator komputer forensik adalah sebuah profesi baru yang sangat dibutuhkan untuk mendukung implementasi hukum pada penanganan cybercrime. Berbagai produk hukum yang disiapkan untuk mengantisipasi aktivitas kejahatan berbantuan komputer tidak akan dapat berjalan kecuali didukung pula dengan komponen hukum yang lain. Dalam hal ini komputer forensik memiliki peran yang sangat penting sebagai bagian dari upaya penyiapan bukti-bukti digital di persidangan.

## PUSTAKA

- [1]. Budhisantoso, Nugroho, Personal Site, alamat: [www.forensik-komputer.info](http://www.forensik-komputer.info)
- [2]. Budiman, Rahmadi, 2003, *Makalah Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa Dan Bagaimana*, Magister Teknik Elektro Option Teknologi Informasi, Institut Teknologi Bandung.2003
- [3]. Kemmish, Rodney Mc., *What is forensic computer*, Australian institute of Criminology, Canberra. Alamat situs: [www.aic.gov.au/publications/tandi/ti118.pdf](http://www.aic.gov.au/publications/tandi/ti118.pdf)
- [4]. Marcella, Albert J., and Robert S. Greenfiled, “*Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes*”, by CRC Press LLC, United States of America. Alamat Situs: [www.forensics-intl.com/def4.html](http://www.forensics-intl.com/def4.html).
- [5]. Shinder, Debra Littlejhon, 2002, *Scene Of Cybercrime, computer forensic hand book*. by Syngress Publishing,Inc.
- [6]. Utdirartatmo, Firar, 2001, *Makalah tugas Tinjauan Analisis Forensik Dan Kontribusinya Pada Keamanan Sistem Komputer*, Magister Teknik Elektro Option Teknologi Informasi, Institut Teknologi Bandung.
- [7]. Wright, Mal, 2001, “*Investigating an Internal Case of Internet Abuse*”, SANS Institute.

## **Literatur Review**

### **I. Fokus Utama Jurnal**

Bagian pendahuluan adalah bagian utama alasan dari sebuah jurnal itu dibuat, pada bagian pendahuluan terdapat point penting yaitu menggambarkan berbagai permasalahan yang timbul karna adanya Cybercrime, kekurangannya terletak pada Teknik Komputer Forensik berdasarkan judul yang diambil. Pada pendahuluan tersebut tidak dibahas apa itu Komputer Forensik dan Kenapa Teknik Komputer Forensik dapat mengantisipasi Cybercrime. Keduanya harus menyatu pada bagian pendahuluan

### **II. Elemen Yang Mempengaruhi Kekuatan Suatu Jurnal**

- Perumusan Masalah  
Tidak mencantumkan Perumusan Masalah yang dapat menjelaskan keterkaitan antara Cybercrime dan Teknik Komputer Forensik, walaupun pada sub yang berbeda ada penjelasan mengenai Cybercrime dan Komputer Forensik
- Metodologi Penelitian  
Jurnal merupakan publikasi dari hasil penelitian yang telah dilakukan bukan merupakan berita atau informasi. Jurnal tersebut hanya memberikan informasi terkait seputar Cybercrime dan cara yang hendak dilakukan tanpa memberikan penjelasan mengenai desain percobaan, peralatan yg digunakan dan jenis pengendaliannya.
- Hasil  
Pada jurnal tersebut tidak mencantumkan hasil-hasil yg dicapai dari Teknik Komputer Jaringan dalam mengatasi Cybercrime. Hasil harus menunjukkan teks-teks bersifat naratif tabel dan gambar yang mudah dimengerti.

### **III. Elemen yang mempengaruhi tingkat kepercayaan suatu jurnal**

- Gaya penulisan
  - Sistematika penulisan tidak tersusun dengan baik
  - Tata bahasa yang dipergunakan dalam penulisan jurnal ini cukup mudah dipahami Meskipun tata letak dari permasalahan yang diambil belum memenuhi kaidah yang sebenarnya dan point-point khusus perlu diperdalam lagi.

## Implementasi Algoritma Enkripsi Playfair pada File Teks

**Rina Chandra Noer Santi**

Program Studi Teknik Informatika  
Fakultas Teknologi Informasi, Universitas Stikubank  
email : r\_candra\_ns@yahoo.com

### Abstrak

Kriptografi berasal dari kata *crypto* yang berarti rahasia dan *graphy* yang berarti tulisan. Jadi kriptografi dapat diartikan sebagai tulisan rahasia. Secara istilah dapat didefinisikan sebagai studi tentang teknik-teknik matematika yang berhubungan dengan keamanan informasi.

Playfair merupakan digraphs cipher, artinya setiap proses enkripsi dilakukan pada setiap dua huruf. Adapun tujuan yang akan di capai adalah membuat aplikasi untuk pengamanan pada file text dengan menggunakan metode Playfair yang dapat mendukung proses perlindungan data yang tidak mudah dicuri dan tidak mudah dipecahkan yang dapat digunakan sebagai keamanan pada data-data yang sangat penting.

**Kata Kunci :** Kriptografi, Enkripsi, *Playfair*, Delphi 6.0

### PENDAHULUAN

Jaringan komputer dan internet telah mengalami perkembangan yang sangat pesat. Teknologi ini mampu menghubungkan hampir semua komputer yang ada di dunia sehingga dapat saling berkomunikasi dan bertukar informasi berupa data teks seperti data keuangan, data user name dan password dari account suatu perusahaan, gambar bergerak, suara maupun email. Seiring dengan perkembangan tersebut, secara langsung ikut mempengaruhi cara berkomunikasi. Jika dahulu untuk berkomunikasi pesan atau surat dengan menggunakan pos, sekarang telah banyak layanan *e\_mail* di internet yang dapat mengirimkan pesan secara langsung kepenerimanya. Akan tetapi sebagai suatu jaringan publik, internet rawan sekali terhadap pencurian data. Maka dan salah satu cara untuk melindungi data dengan menggunakan seni Kriptografi.

#### Pengertian Kriptografi

Secara bahasa Kriptografi berasal dari kata *crypto* yang berarti rahasia dan *graphy* yang berarti tulisan. Jadi kriptografi dapat diartikan sebagai tulisan rahasia. Secara istilah dapat didefinisikan sebagai studi tentang teknik-teknik

matematika yang berhubungan dengan keamanan informasi.

Teknik kriptografi terdiri dari simetri dan asimetri. Teknik ini digunakan untuk mengamankan aplikasi (keamanan informasi) sehingga dapat menjaga kerahasiaan, integritas data, autentikasi data dan *non-repudiation*

Kriptografi diperlukan karena pada dasarnya informasi sangat penting bagi segala aspek, tuntutan keamanan informasi berubah dari waktu ke waktu. Perubahan tuntutan ini terjadi karena transformasi atau penggunaan perlengkapan kebutuhan utama untuk pertukaran informasi, dari mulai cara tradisional (fisik) yang membutuhkan mekanisme pengarsipan atau administrasi secara fisik dan membutuhkan ruang yang lebih besar, menggunakan otomatisasi komputer personal, sampai transfer informasi melalui penggunaan jaringan komputer, baik intranet maupun internet yang sekarang menjadi tren dan kebutuhan.

Kriptografi secara umum merupakan ilmu dan seni untuk menjaga kerahasiaan berita (*Bruce Schneier–Applied Cryptography*). Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi

seperti kerahasiaan data, keabsahan data, integritas data, serta Otentikasi data (A. Menezes, P. Van Oorschot and S. Vanstone—Handbook of Applied Cryptography). Namun, pada kriptografi tidak semua aspek keamanan informasi akan ditangani.

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi adalah :

#### 1. Kerahasiaan (*Confidentiality*)

Adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.

#### 2. Integritas Data (*Data Integrity*)

Berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk dapat menjaga integritas data, suatu sistem harus memiliki kemampuan untuk mendeteksi manipulasi data yang dilakukan pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pendistribusian data lain ke dalam data yang asli.

#### 3. Otentifikasi (*Authentication*)

Berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diOtentikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.

#### 4. Non-repudiasi (*Non-repudiation*)

Merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat.

### Algoritma Kriptografi

Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua golongan, yaitu :

#### a. Algoritma Simetris (*Symmetric Algorithms*)

Dalam *Symmetric Algorithms* ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik  $K_1 = K_2 = K$ , tetapi satu buah kunci dapat pula diturunkan dari

kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Jumlah kunci yang dibutuhkan umumnya:

$$C = \frac{n \cdot (n-1)}{2}$$

dengan  $n$  = menyatakan banyaknya pengguna (user)

$C$  = menyatakan banyaknya kunci.

Tingkat keamanan kriptosistem yang menggunakan algoritma ini sangat ditentukan oleh kerahasiaan kunci  $K$  yang digunakan. Jika seseorang hendak mengirimkan suatu pesan kepada orang lain, atau melakukan secure communication, orang tersebut harus terlebih dahulu memberikan kepada pihak yang dituju kunci  $K$  yang hendak digunakannya. Hal ini jelas membutuhkan saluran komunikasi yang benar-benar aman dan tidak dapat disadap (*secure channel*).

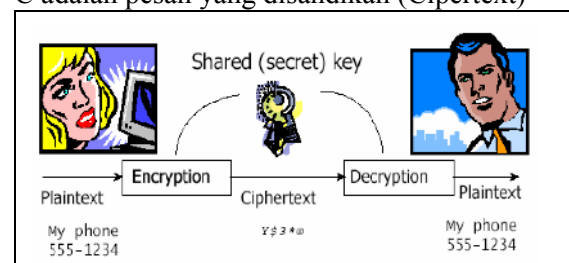
Secara matematis Algoritma ini dapat ditulis :

$$E_k(M) = C \quad d_k(C) = M$$

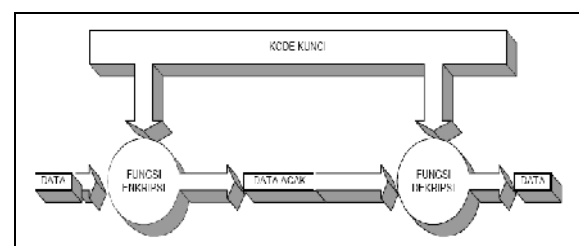
$E_k$  adalah proses enkripsi dengan menggunakan kunci  $K$

$M$  adalah pesan asli (Plaintext)

$C$  adalah pesan yang disandikan (Ciphertext)



Gambar 1. Algoritma Simetris (*Symmetric Algorithms*)



Gambar 2. Teknik Algoritma Simetris (*Symmetric Algorithms*)



Prinsip kerja dari kriptografi kunci simetrik adalah sebagai berikut :

1. Pengirim dan penerima data atau Informasi sepakat menggunakan system kriptografi tertentu
2. Pengirim dan penerima sepakat menggunakan satu kunci tertentu
3. Dilakukan enkripsi sebelum data dikirim dan dekripsi setelah data dikirim

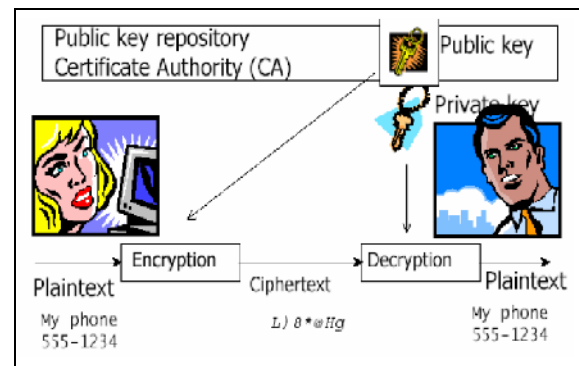
Tingkat keamanan dari kriptosistem yang menggunakan algoritma ini sangat ditentukan oleh kerahasiaan kunci K yang digunakan. Jika seseorang hendak mengirimkan suatu pesan kepada orang lain atau melakukan *secure communication*, orang tersebut harus terlebih dahulu memberitahu kepada pihak yang dituju kunci K yang digunakannya. Hal jelas membutuhkan saluran komunikasi yang benar-benar aman tidak data disadap (*secure channel*). Faktor inilah yang menjadi kelemahan cara ini yaitu masalah keamanan kunci dan bagaimana mendistribusikan kunci K tersebut.

#### b. Algoritma Asimetri (*Asymmetric Algorithms*)

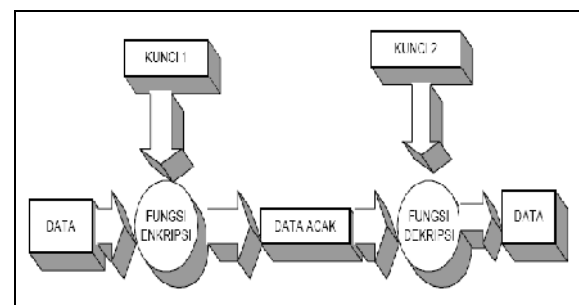
Dalam *Asymmetric Algorithms* ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

Setiap *cryptosystem* yang baik harus memiliki karakteristik sebagai berikut :

1. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.



Gambar 3. Algoritma Asimetri (*Asymmetric Algorithms*)



Gambar 4. Algoritma Asimetri (*Asymmetric Algorithms*)

3. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
4. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

Namun demikian perlu diperhatikan bahwa bila suatu *cryptosystem* berhasil memenuhi seluruh karakteristik di atas belum tentu ia merupakan sistem yang baik. Banyak *cryptosystem* lemah yang terlihat baik pada awalnya. Kadang kala untuk menunjukkan bahwa suatu *cryptosystem* kuat atau baik dapat dilakukan dengan menggunakan pembuktian matematika. Hingga saat ini masih banyak orang yang menggunakan *cryptosystem* yang relatif mudah dibuka, alasannya adalah mereka tidak mengetahui sistem lain yang lebih baik serta kadang kala terdapat motivasi yang kurang untuk menginvestasikan seluruh usaha yang diperlukan untuk membuka suatu system.

#### Sandi Playfair

Sandi Playfair digunakan oleh Tentara Inggris pada saat Perang Boer II dan Perang

Dunia I. Ditemukan pertama kali oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tanggal 26 Maret 1854. Playfair merupakan digraphs cipher, artinya setiap proses enkripsi dilakukan pada setiap dua huruf. Misalkan plainteksnya “KRIPTOLOGI”, maka menjadi “KRIPTOLOGI”. Playfair menggunakan tabel 5x5. Semua alfabet kecuali J diletakkan ke dalam tabel. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil. Kunci yang digunakan berupa kata dan tidak ada huruf sama yang berulang. Apabila kuncinya “MATAHARI”, maka kunci yang digunakan adalah “MATHRI”. Selanjutnya, kunci dimasukkan ke dalam tabel 5x5, isian pertama adalah kunci, selanjutnya tulis huruf-huruf berikutnya secara urut dari baris pertama dahulu, bila huruf telah muncul, maka tidak dituliskan kembali.

Tabel 1. Kunci Matahari

M	A	T	H	R
I	B	C	D	E
F	G	K	L	N
O	P	Q	S	U
V	W	X	Y	Z

Berikut ini aturan-aturan proses enkripsi pada Playfair yaitu

1. Jika kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan yang sekolom dengan huruf pertama. Contohnya, SA menjadi PH, BU menjadi EP.
2. Jika kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf setelahnya dalam baris yang sama, demikian juga dengan huruf kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, AH menjadi TR, LK menjadi KG, BE menjadi CI.
3. Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, DS menjadi LY, PA menjadi GW, DH menjadi HY.
4. Jika kedua huruf sama, maka letakkan sebuah huruf di tengahnya (sesuai kesepakatan).
5. Jika jumlah huruf plainteks ganjil, maka tambahkan satu huruf pada akhirnya, seperti pada aturan ke-4.






Sedangkan proses dekripsinya adalah kebalikan dari proses enkripsi. Contohnya, HR didekrip menjadi HT, BS didekrip menjadi DP, ZU didekrip menjadi RZ.

## HASIL IMPLEMENTASI

### Form Enkripsi



Gambar 5. Form Enkripsi

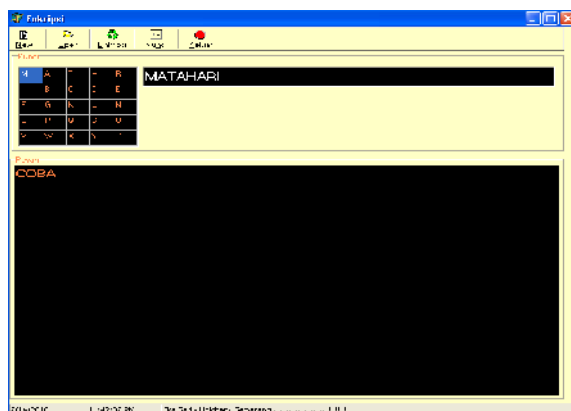
Pada form enkripsi terdapat 5 tombol yang dapat digunakan yaitu tombol  yang digunakan untuk membuka file baru yang akan di enkripsi, tombol  yang digunakan untuk membuka file yang akan dienkripsi, tombol  yang digunakan untuk melakukan enkripsi file dengan menggunakan metode playfair, tombol  yang digunakan untuk membuat kunci dengan bentuk tabel 5 x 5 secara otomatis dan tombol  yang digunakan untuk keluar dari program enkripsi.

Pada proses enkripsi, program akan membuat kunci kriptografi dengan sandi (“MATAHARI”) dengan ukuran tabel 5 x 5. Pada metode playfair kunci yang dimasukkan tidak boleh ada kata yang berulang dan semua huruf kecuali J tidak dimasukkan ke dalam tabel sehingga jika menggunakan kunci “MATAHARI” maka akan menjadi “MATHRI”. Selanjutnya, kunci dimasukkan ke dalam tabel 5x5 dimana isian pertama adalah kunci, selanjutnya tulis huruf-huruf berikutnya secara urut dari baris pertama dahulu, bila huruf telah muncul, maka tidak dituliskan kembali sampai tabel terisi semua.

Tabel 2. Kunci “MATAHARI”

M	A	T	H	R
I	B	C	D	E
F	G	K	L	N
O	P	Q	S	U
V	W	X	Y	Z

Setelah itu, program akan mengelompokkan pesan (“coba”) yang akan dienkripsi yang terdapat pada komponen richedit masing-masing menjadi 2 huruf dan membuat semua karakter menjadi huruf besar (*upper case*) dan menyimpan ke dalam array tmp1 dengan urutan sebagai berikut:



Gambar 6. Pesan Enkripsi “coba”

Tmp1[0] : = CO

Tmp1[2] : = BA

Setelah itu program akan melakukan pengecekan sesuai dengan metode enkripsi playfair dimana :

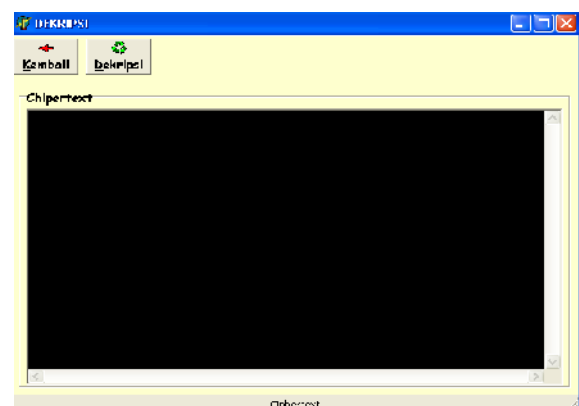
1. Jika kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf
2. Jika kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf setelahnya dalam baris yang sama, demikian juga dengan huruf kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua.
3. Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua.

pesan ciphertext sebagai berikut :

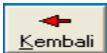

1. Pesan “CO” tidak terletak pada baris dan kolom yang sama sehingga masuk ke aturan playfair enkripsi no 1, sehingga pesan “CO” menjadi C = “IQ”
2. Pesan “BA” terletak pada kolom yang sama sehingga masuk ke aturan playfair enkripsi no 3, sehingga pesan “BA” menjadi C = “GB”

Sehingga program akan mengenkripsi pesan “coba” dengan ciphertext ”IQGB”

### Proses Dekripsi



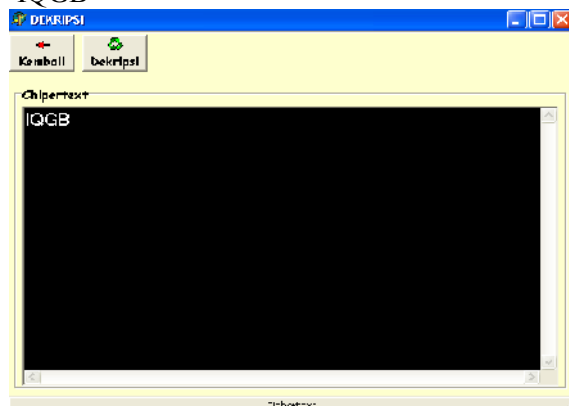
Gambar 7. Form Dekripsi

Pada proses dekripsi terdapat 2 tombol yang dapat digunakan yaitu tombol  yang digunakan untuk kembali ke form enkripsi dan menutup form dekripsi, tombol  yang digunakan untuk melakukan proses dekripsi file yang telah dienkripsi.

Pada proses dekripsi kebalikan dengan proses enkripsi dengan ketentuan dekripsi playfair sebagai berikut :

1. Jika kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan sekolom dengan huruf pertama.
2. Jika kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf sebelumnya dalam baris yang sama, demikian juga dengan huruf kedua. Jika terletak pada baris kesatu, maka menjadi baris kelima, dan sebaliknya.
3. Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf sebelumnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika terletak pada kolom pertama, maka menjadi kolom kelima, dan sebaliknya.

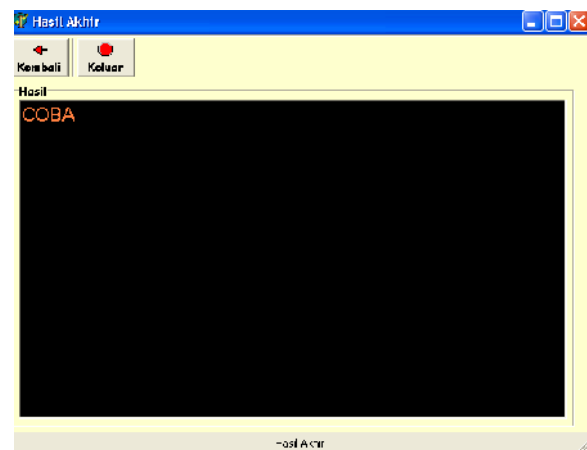
Pada proses dekripsi program akan melakukan pencarian pesan dan mengelompokkan menjadi 2 huruf yang dienkripsi dan menyimpan ke dalam array tmp1. Pesan "coba" dienkripsi menjadi ciphertext "IQGB"





Gambar 8. Pesan Enkripsi "COBA"

1. Pesan "IQ" tidak terletak pada baris dan kolom yang sama sehingga masuk ke aturan playfair dekripsi no 1, sehingga pesan "IQ" menjadi M = "CO"
2. Pesan "GB" terletak pada kolom yang sama sehingga masuk ke aturan playfair dekripsi no 3, sehingga pesan "GB" menjadi M = "BA"

Sehingga akan didapatkan pesan "COBA" dan pesan setelah didekripsi sama pada saat pesan sebelum dienkripsi



Gambar 9. Hasil Dekripsi

Pada form hasil akhir terdapat 2 tombol yang dapat digunakan yaitu tombol  yang digunakan untuk kembali ke form dekripsi dan tombol  untuk menutup form hasil dan kembali ke form utama.

" COBA LAGI DEH "  
Dengan kunci " MATAHARI"

	1	2	3	4	5
1	M	A	T	H	R
2	I	B	C	D	E
3	F	G	K	L	N
4	O	P	Q	S	U
5	V	W	X	Y	Z

Plaintext	CO	BA	LA	GI	DU	LU
-----------	----	----	----	----	----	----

Baris	24	21	31	32	24	34
-------	----	----	----	----	----	----

Kolom	31	22	42	21	45	45
-------	----	----	----	----	----	----

### Di Enkripsi

Chypertext	IQ	GB	GH	FB	ES	NS
------------	----	----	----	----	----	----

Baris	24	32	31	32	24	34
-------	----	----	----	----	----	----

Kolom	13	22	24	12	54	54
-------	----	----	----	----	----	----

### PENUTUP

#### Kesimpulan

- Program aplikasi kriptografi ini akan membatasi orang yang tidak berhak atas informasi atau data yang dimiliki oleh si pengirim untuk dibaca karena pesan sudah dienkripsi dan dapat menjaga kerahasiaan pesan atau informasi file-file yang ada dalam sebuah komputer.
- Pembuatan teknik kriptografi enkripsi dekripsi dengan menggunakan metode playfair dapat melindungi data dimana program akan melakukan proses enkripsi hanya berupa huruf dengan menggunakan tabel 5 X 5.

### DAFTAR PUSTAKA

- Elka ,Lab, 2001, *Pelatihan Delphi*, [www.planck.fi.itb.ac.id](http://www.planck.fi.itb.ac.id)
- Jogiyanto.HM, 2002, *Analisis dan Desain Sistem Informasi*, Andi Offset, Yogyakarta.
- Kadir,Abdul, 2001, *Dasar Pemrograman Delphi 6.0*, Andi Offset, Yogyakarta.
- Mahyusir,Tavri D. 2002, *Pengantar Analisis dan Perancangan Perangkat Lunak*, Andi Offset, Yogyakarta
- Mahyusir,Tavri D 1991, *Pengantar Analisis dan Perancangan Perangkat Lunak*, Andi Offset,Yogyakarta.

Munir,Rinaldi, 2006, *Diktat Kuliah IF5054 Kriptografi*, Institut Teknologi Bandung, Bandung.

Musalini,Uus 2004, *Membangun Aplikasi Super Cantik Dan Full Animasi Dengan Delphi*, PT. Elex media Computindo, Jakarta

Pressman ,Roger S, 2002, *Rekayasa Perangkat Lunak*, Andi Offset,Yogyakarta

Riyanto,M Zaki, 2008, *Kriptografi Pada Perang Dunia I : Sandi Playfair*, <http://zaki.math.we.id>, Yogyakarta.

Sisyboy, 2004, *Flowchart dan Source Code RSA*, <http://sisyboy.files.wordpress.com/2008/01/flowchart.doc>

Whitten ,Jeffery L., 2004, *Metode Desain dan Analisa Sistem*, Andi Offset, Yogyakarta

46goenk, 2008, *RSA Algorithm*, <http://agcrypt.wordpress.com/2008/02/25/rsa-algorithm/>

## Literatur Review

### I. Ferokus Utama Jurnal

Pada bagian Pendahuluan hanya mencantumkan permasalahan yang bersifat global atau umum, alangkah baiknya jika diberikan Latar Belakang permasalahan yang bisa menggambarkan menggunakan Implementasi Algoritma Enkripsi Playfair atau tanpa menggunakan Implementasi Algoritma Enkripsi Playfair

### II. Elemen Yang Mempengaruhi Kekuatan Suatu Jurnal

- Perumusan Masalah  
Implementasi Algoritma Enkripsi Playfair seperti yang jelaskan pada jurnal diatas terlihat memiliki power yang kuat untuk merahasiakan data, namun Tidak mencantumkan Perumusan Masalah yang dapat menjelaskan perbandingan antara algoritma yang diambil dengan algoritma lain karna kemungkinan algoritma yang lain akan lebih super power
- Metodologi  
Alangkah baiknya Metodologi dibuatkan sub terpisah yang ditandai angka atau abjad agar mudah dimengerti dan tidak menyatu seperti jurnal diatas yang terkesan membingungkan
- Hasil  
Pada jurnal tersebut mencantumkan hasil-hasil dicapai dan memberikan penjelasan yang dapat dimengerti dan dapat mempengaruhi kekuatan suatu jurnal

### III. Elemen yang mempengaruhi tingkat kepercayaan suatu jurnal

- Gaya penulisan
  - Sistematika penulisan tidak tersusun dengan baik
  - Tata bahasa yang dipergunakan dalam penulisan jurnal ini cukup mudah dipahami meskipun tata letak perlu mengikuti kaidah-kaidah jurnal dan alangkah baiknya diberikan sub-sub yang ditandai dengan angka atau abjad

## KONSEP SOLUSI KEAMANAN WEB PADA PEMOGRAMAN PHP

**KM. Syarif Haryana**

STMIK Mardira Indonesia, Bandung 40235  
kmsyarifharyana@yahoo.co.id

### ***Abstract***

*PHP is an open source application and has the global auto facility on variables where each programmer is given the ease to apply. But this also facilitates ease attacker to destroy each program run . This attack can be avoided (minimized) by conducting safety. This paper will examine various aspects of the potential sources of easily disturbed security on PHP scripts and create alternative solutions workarounds.*

*In addition it also presented several vulnerabilities in the web in general and especially on the web are built using PHP scripts. Including some of the techniques that are usually used by intruders to download deface a web page.*

*At the end of the section presented several alternative solutions of various levels of information security including application level. The concept of web security solutions are a few web pages business owners , managers or administrators of web pages for secure web server and perform information security measures . Although the information security must be comprehensively and continuously due process deface web pages will be done when the inadvertence of the person in charge of the web page.*

**Keywords:** *autoglobal, attacker, vulnerability, deface*

### **Abstrak**

PHP adalah aplikasi yang open source dan mempunyai fasilitas *auto global* pada variabel dimana setiap programer diberikan kemudahan untuk mengaplikasikannya. Tetapi kemudahan ini pula yang memudahkan attacker untuk merusak setiap program dijalankan. Serangan ini dapat dihindari (diminimalkan) dengan cara mengadakan pengamanannya. Untuklah tulisan ini akan mengkaji berbagai sumber tentang aspek potensial yang mudah diganggu keamanannya pada script PHP dan membuat alternatif solusi penangannya.

Selain itu dipaparkan pula beberapa vulnerability pada web umumnya dan khususnya pada web yang dibangun dengan menggunakan skrip PHP. Termasuk beberapa teknik-teknik yang biasanya digunakan oleh para penyusup untuk men-*deface* sebuah halaman web.

Pada bagian akhir dipaparkan beberapa alternatif pemecahan dari berbagai level keamanan informasi termasuk dari level aplikasi. Konsep solusi keamanan web

merupakan beberapa usaha pemilik halaman web, pengelola halaman web atau para admin web server untuk mengamankan dan melakukan langkah-langkah pengamanan informasi. Meskipun pengamanan informasi tersebut harus dilakukan secara komperhensif serta berkesinambungan karena proses *deface* halaman web akan dilakukan ketika terjadi kelengahan para penanggung jawab halaman web.

**Kata Kunci:** *Autoglobal, Attacker, Vulnerability, Deface*

### A. PENDAHULUAN

Keamanan Web menjadi lebih lagi dibutuhkan dengan adanya kasus-kasus pencurian melalui Web, penipuan, perusakan, virus, worm, dan lain-lain. Karena pentingnya masalah kewanamanan ini maka bagi setiap orang yang ingin mengembangkan Webnya sudah selayaknya mempersiapkan diri sebaik-baiknya. Apalagi jika dalam pengembangan Web akan digunakan untuk aplikasi-aplikasi yang rentan atau kritis, maka kewanamanan yang baik akan menghindarkan kerugian yang mungkin didapat yang jumlahnya mungkin bisa sangat besar, baik secara material maupun nonmaterial.

### B. ANALISIS MASALAH

Sebagai konsekuensi kepraktisan dan kemudahannya, instalasi default PHP banyak memiliki kelemahan keamanan. Variabel global di PHP dapat berasal dari masukan pengunjung Web (dari GET/POST/Cookie), sehingga bila programernya ceroboh tidak melakukan inisialisasi tiap variabel sebelum pemakaian, seorang penyerang dapat memasukkan nilai-nilai awal variabel ke dalam skrip untuk mengubah kelakuannya. Sebelum PHP 3.0.18 terdapat bug pada file upload yang banyak dieksploitasi untuk menembus banyak situs PHP. Dalam bug ini interpreter PHP dapat diakali untuk menulis file di filesystem server mana pun sesuai keinginan penyerangnya,

karena path dapat dimasukkan lewat form HTML.

Beberapa kelemahan ini dapat dikonfigurasi atau dimatikan. Karena itu seorang programmer PHP dan admin perlu mengetahui opsi-opsi konfigurasi PHP agar sistem mereka lebih aman.

### C. LUBANG KEAMANAN PHP

PHP dapat dijalankan sama seperti aplikasi CGI (*Common Gateway Interface*) seperti web server yang terintegrasi. Interpreter PHP mempunyai kemampuan untuk mengakses hampir semua *host-file system, network interfaces, IPC*, dan lain-lain. Konsekwensinya PHP potensial mendapat serangan dari attacker. Untuk meminimalkan serangan programmer harus menyadari dan mengetahui hal-hal yang tidak diharapkan (merusak) saat program dijalankan, yaitu pengetahuan kelemahan suatu sistem dan modus serangan secara umum yang diarahkan untuk mengganggu keamanan program tersebut. Lubang keamanan yang paling umum di dalam skrip PHP dan tak terkecuali pada aplikasi web yang manapun, adalah berkaitan dengan *User Input*. Banyak skrip menggunakan informasi *user* yang legal dalam bentuk format web dan memproses informasi ini dengan berbagai cara. Jika *user input* ini dilegalkan tanpa batasan, maka *user input* potensial menyisipkan perintah-perintah yang tidak diinginkan dalam skrip.



### SQL Injections

Selain itu metode SQL Injections banyak pula digunakan untuk memanfaatkan kelemahan pada mesin server SQLnya, misalnya server yg menjalankan aplikasi tersebut. Hal ini dilakukan dengan mencoba memasukkan suatu script untuk menampilkan halaman error di browser, dan biasanya halaman error akan menampilkan *paling tidak* struktur dari hirarki server dan logika program. Metode ini memasukan “karakter” query tertentu pada sebuah “text area” Trend keamanan dan Serangan komputer| ver 1 atau di address browser dengan perintah-perintah dasar SQL seperti SELECT, WHERE, CREATE, UPDATE, dan lain-lain.

### Cross site script (XSS)

Type lubang keamanan sistem lainnya yang biasa ditemukan di *web based applications* dengan melakukan *code injections* dengan malicious web pengguna kepada halaman web yang dilihat oleh user lainnya dimana memungkinkan penyerang untuk mencuri cookies, menipu user dengan memberikan credentials mereka, memodifikasi penampilan page, mengeksekusi seluruh sort dari malicious javascript code

### Web Spoofing

- Web Spoofing
  - Membuat web lain yang “*copy paste/identik*” dari web asli – Membeli domain yang hampir identik
  - Ex : klikbca.com (existing)
  - Lalu dibeli domain klikbca.com / clickbca.com / clickbca.net
  - Menangkap user dan password

### Penanganan

- Digital Certificate
- Verisign, iTrust, ...
- CA (Certificate Authority)
- https

### D. PEMBAHASAN

#### KONSEP/SOLUSI

Dari beberapa vulnerabilities pemograman aplikasi berbasis PHP yang telah di paparkan di atas, maka dapat diusulkan beberapa konsep solusi, yaitu :

#### Validasi Login

Tulisan ini diperuntukan bagi para newbie yang ingin membuat system login pada webnya dengan php. Apa yg akan dipaparkan berikut ini sebenarnya sangat umum dan dapat diperoleh dari berbagai sumber yang berhubungan dengan php. Berikut ini hal-hal yang harus kita pertimbangkan ketika membuat login:

1. Pastikan form login adalah form dari server kita.
2. Amankan input text untuk user dan password, metoda dan format data.
3. Hindari penggunaan register global (untuk php v 4.2.0 keatas sudah disable).
4. Expired time dari login yang dilakukan.
5. Pastikan file yang tidak boleh diakses tidak dapat dipanggil secara langsung.

Di bawah ini salah contoh satu logika dari banyak kemungkinan. Logika ini akan sangat beragam jadi bukanlah satu-satunya cara ataupun cara yang paling baik.

- Saat membuat form login (misalnya: index.php) sebagai default kita mulai dengan membuat session baru.
- Session\_name disini sebagai referensi untuk session id di cookies dan URL.

Daftarkan suatu variabel session baru SES\_TOKEN dengan memakai fungsi session\_register.

- Buat token berupa kata acak yang akan kita gunakan untuk memastikan form adalah dari kita.

- Lalu Enkrip token agar lebih rumit. (Pada dasarnya token ini mirip dengan session id)
- Tambahkan variabel enkrip token tersebut dalam form melalui hidden.

Misalnya pada file "cekmasuk.php" kita lakukan pemeriksaan apakah data yang kita terima dari form yang kita buat sebelumnya. Amankan input text untuk user dan password, metoda dan format data. Pada saat kita menerima data maka sebelum kita olah misalnya untuk kasus user dan password, maka harus kita pastikan data tersebut tidak disisipi niat jahat. Untuk itu maka kita buat suatu fungsi filter. Hindari penggunaan register global (untuk php v 4.2.0 ke atas sudah disable/off).

Untuk hal ini kita dapat memperoleh data yang dikirim melalui predefine variabel milik php, yaitu:  
`$HTTP_GET_VARS`  
 untuk metoda get  
`$HTTP_POST_VARS`  
 untuk metoda post.

Expired Time dari login yang dilakukan. Setiap login yg dilakukan user sering kali mereka tidak melakukan logout, hanya mendingkan atau malah meninggalkan ketika masih login. Oleh karena itu expired time ini adalah wajib dalam sistem login.

### SQL Injection

#### Hilangkan Karakter-Karakter *Escape* dalam Perintah SQL

Kesalahan umum yang terjadi adalah penggunaan nilai variabel yang disediakan oleh *user* atau URL dalam sebuah *query* SQL tanpa menghilangkan karakter-karakter khusus. Perhatikan contoh kode fragmen berikut dari sebuah skrip yang dirancang untuk mengecek kebenaran *username* dan *password* yang dimasukkan dalam halaman HTML:  
`$query = "SELECT * FROM users  
 WHERE username=' " . $username`

```
. " " AND password=' " .  

$password . " " " ;  

// record yang memenuhi  

perintah di atas terdapat di  

suatu tempat  

if (record_exists($query)) {  

  echo "Access granted";  

} else {  

  echo "Access denied";  

}
```

Perintah ini akan jalan jika pengaksesan menggunakan `check.php?user name=admin&password= x`. Akan tetapi, jika kode ini diakses dengan menggunakan `check.php?username=admin&password=a%27+OR+1%3Di%271` (dan jika `magic_quotes_gpc` dibuat *disabled*) maka `password` akan menjadi `Password='a' or 1='1'` sehingga *record* pengguna *admin* akan selalu dikembalikan berapapun nilai `password`.

### Penggunaan HTTPS Protokol

Solusi selanjutnya kita dapat pergunakan protokol yang dapat mendukung segi keamanan yaitu https. **HTTPS** (HTTP melalui SSL or HTTP Secure), merupakan protokol HTTP yang menggunakan Secure Socket Layer (**SSL**) atau Transport Layer Security (TLS) sebagai sub layer dibawah HTTP aplikasi layer yang biasa. HTTP di enkripsi dan deskripsi dari halaman yang diminta pengguna serta halaman yang dikembalikan oleh web server. HTTPS digunakan untuk melindungi dari orang mengakses tanpa izin dan dari serangan *man-in-the-middle*. HTTPS dikembangkan oleh Netscape.

Dengan HTTPS kita dapat melakukan proteksi data yaitu hanya penerima saja yang dapat membaca data, Kenyamanan (data privacy), memungkinkan identifikasi server ataupun client, otentikasi server dan klien, dan integritas data. Sedangkan **SSL** (Secure Socket Layer) adalah arguably internet

yang paling banyak digunakan untuk enkripsi. Ditambah lagi, SSL digunakan tidak hanya keamanan koneksi web, tetapi untuk berbagai aplikasi yang memerlukan enkripsi jaringan end-to-end.

### HTTPS, TLS, and SSL

**Https** adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektrik. Pendekatan HTTPS sangatlah simpel, Client membuat koneksi ke server, melakukan negosiasi koneksi SSL, kemudian mengirim HTTP tersebut melalui aplikasi SSL. Deskripsi ini menjadikannya terlihat mudah. Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers, dan man in the middle attacks.

Pada umumnya port HTTPS adalah 443. Terdapat perbedaan *port* yang spesifik, HTTPS menggunakan *port* 443 sedangkan HTTP menggunakan *port* 80 dalam berinteraksi dengan *layer* yang dibawahnya, TCP/IP/ HTTPS dan SSL mendukung penggunaan dari X.509 sertifikat digital dari server, sehingga jika diperlukan, pengguna dapat mengotentikasi pengirimnya. Kecuali perbedaan *port* yang spesifik, HTTPS menggunakan *port* 443 sedangkan HTTP menggunakan *port* 80 dalam berinteraksi dengan *layer* yang dibawahnya, TCP/IP/ Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithm penyangkian yang aktual. Oleh karena itu, pada halaman web digunakan HTTPS, dan

URL yang digunakan dimulai dengan 'https://' bukan dengan 'http://'. Efektifitas dari HTTPS dapat dibatasi oleh kurangnya implementasi dari browser atau perangkat lunak server atau kurangnya dukungan dari beberapa algoritma.

Selanjutnya, walaupun HTTPS dapat mengamankan perjalanan data antara server dan klien, setelah data didekripsi tujuannya, itu hanya aman sebagai *host* komputer. Kesalahpahaman yang sering terjadi pada pengguna kartu kredit di web ialah dengan menganggap HTTPS "sepenuhnya" melindungi transaksi mereka. Sedangkan pada kenyataannya, HTTPS hanya melakukan enkripsi informasi dari kartu mereka antara browser mereka dengan web server yang menerima informasi. Pada web server, informasi kartu mereka secara tipikal tersimpan di database server (terkadang tidak langsung dikirimkan ke pemroses kartu kredit), dan server database inilah yang paling sering menjadi sasaran penyerangan oleh pihak-pihak yang tidak berkepentingan.

### E. KESIMPULAN

Kesimpulan yang dapat diambil dari pembahasan makalah ini antara lain sebagai berikut:

1. Teknologi Web server merupakan inti setiap desain aplikasi Web. Tanpa memberi perhatian khusus pada keamanannya, konfigurasi defaultnya justru akan menjadi sejumlah jalan penyerangan bagi para penyerang. Konfigurasi default biasanya memberikan berbagai kemudahan dan fitur tambahan, namun tidak selalu diperlukan. Untuk itu perlu diperhatikan sekali lubang keamanannya.
2. Dalam mengembangkan aplikasi Web, sangat penting untuk dipahami bagaimana kerja masing-masing teknologi Web yang dipakai

agar dapat diantisipasi kelemahan-kelemahan keama-nannya. Seperti :

- Programming Language Vulnerabilities (PHP, .NET)
  - SQL Injections of hostile SQL commands allow attackers to steal data
  - Cross-Site Scripting Exploits allow attackers to insert hostile content from domains that they control.
3. Mengapa HTTPS :
- Melindungi data dari akses yang tidak diijinkan, hanya penerima yang diijinkan untuk membaca data
  - Menjaga kerahasiaan data (data privasi).
  - Integritas data
  - Klien dan server autentikasi
  - Memastikan bahwa tidak ada yang bisa merusak data yang ditransmisikan.

## DAFTAR PUSTAKA

- Clancy Malcolm, *Ten Security Check For PHP*, Website, [http://www.onlamp.com/pub/a/php/2003/03/20/php\\_security.htm](http://www.onlamp.com/pub/a/php/2003/03/20/php_security.htm)
- Jordan Dimov, *On The Security Of PHP*, Website : <http://www.developer.com/lang/php/article.php/922871>
- Sufehmi, Harry, *Security di PHP*, Website <http://www.tf.itb.ac.id/~eryan/Php/PHPSecurity.txt>
- John Coggeshall, *PHP Security*, Website <http://www.onlamp.com/pub/au/135>
- Kadir, Abdul, *Dasr Penmrograman Web Dinamis Menggunakan PHP*, Andi, Yogyakarta, 2002.
- An ISS Technical White Paper, Web Application Protection

## **Literatur Review**

### **I. Fokus Utama Jurnal**

- Bagian Pendahuluan dapat mewakili dari permasalahan yang dihadapi, namun perlu ditambahkan kata – kata solusi gara terdapat keseimbangan antara masalah yang dijelaskan dengan solusi yang ditawarkan.

### **II. Elemen Yang Mempengaruhi Kekuatan Suatu Jurnal**

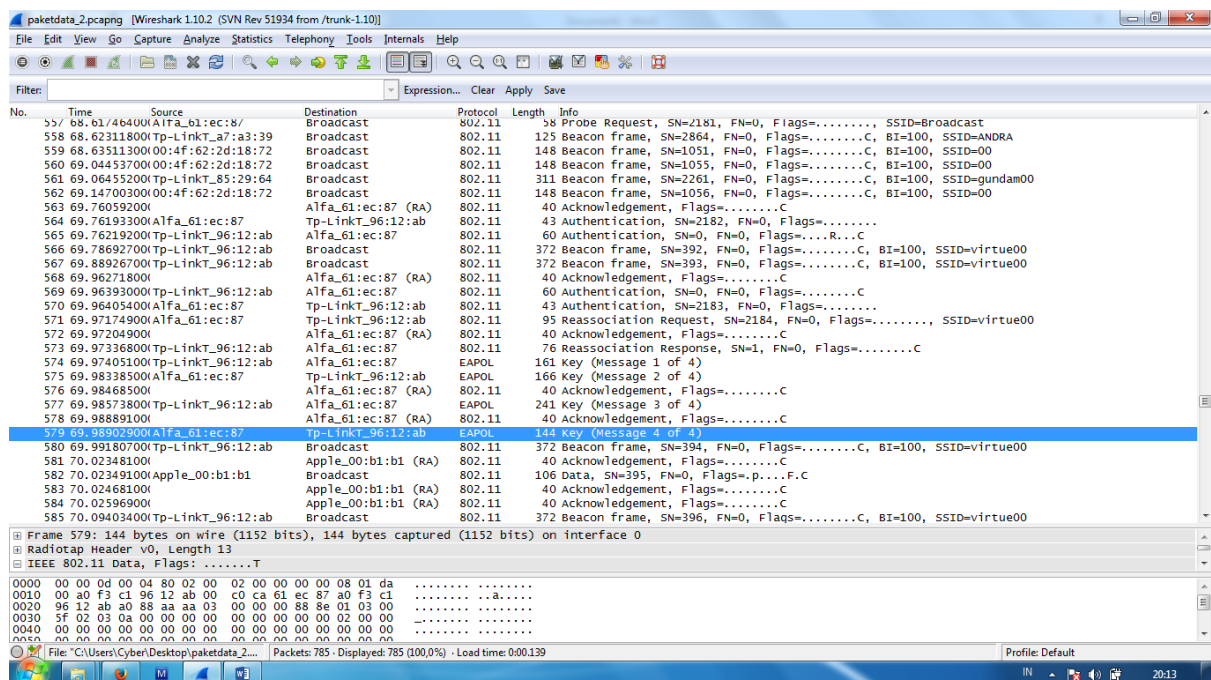
- Perumusan Masalah  
Dari Analisis Masalah yg dijelaskan terdapat Perumusan Masalah yang dapat mempengaruhi kekuatan jurnal
- Metodologi  
Metodologi lebih baik ditempatkan pada sub tersendiri agar mudah dipahami
- Hasil  
Hasil yang diperoleh dapat mempengaruhi kekuatan suatu jurnal.

### **III. Elemen yang mempengaruhi tingkat kepercayaan suatu jurnal**

- Gaya penulisan
  - Sistematika penulisan tersusun dengan baik
  - Tata bahasa yang dipergunakan dalam penulisan jurnal ini cukup mudah dipahami dan mengikuti kaidah-kaidah jurnal

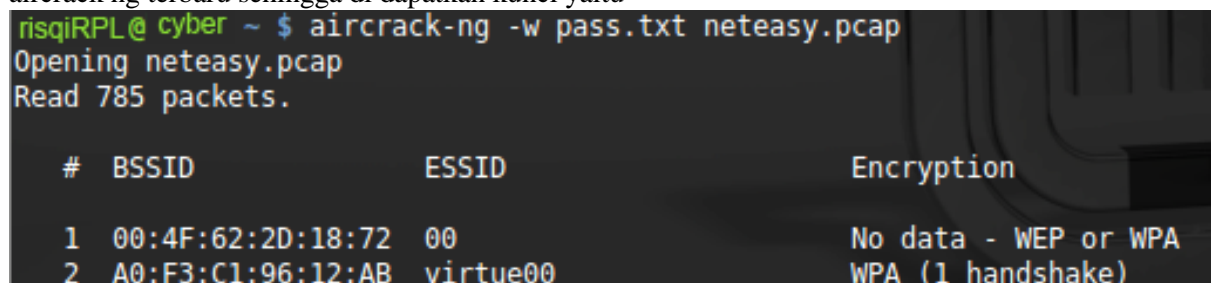
## 2. Langkah-langkah untuk menemukan "sesuatu" yang tersembunyi pada file pcap

Disini saya menggunakan Wireshark, Paket EAPOL itu yang berusaha ngecrack soalnya di manual penggunaan/ help software Wireshark untuk mengecrack sebuah keamanan WPA memerlukan 4 jalan di wiresharknya yang tertulis 4 adalah paket EAPOL



Setelah itu di cari yang nama wifi yang menggunakan WPA, dari 5 ssid yang menggunakan WPA adalah virtue00

Habis itu di crack dengan backtrack versi r3 dan dictionarynya menggunakan wordlist dengan aircrack ng terbaru sehingga di dapatkan kunci yaitu



# idsecconf2013