**KEAMANAN SISTEM INFORMASI**

**PENDALAMAN MATERI DAN KASUS KEAMANAN SISTEM INFORMASI**

****

MATA KULIAH : KEAMANAN SISTEM INFORMASI

**DISUSUN OLEH :**

**ADELLA FITRI SETIANDA**

**17670025**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS TEKNIK DAN INFORMATIKA**

**UNIVERSITAS PGRI SEMARANG**

**2020**

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

Kriptografi berasal dari bahasa Yunani dengan memadukan dua kata, yaitu kryptos dan graphein. Kryptos berarti tersembunyi atau rahasia, sedangkan graphein memiliki arti menulis. Makna kriptografi secara harfiah ialah menulis secara tersembunyi untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaannya. Kriptorafi memiliki pengertian lain, yakni suatu ilmu tentang teknik enkripsi naskah asli (plaintext) yang diacak memanfaatkan sebuah kunci enkripsi sehingga naskah asli tersebut berubah menjadi naskah yang sulit dibaca (chipertext) oleh pihak yang tidak memiliki kunci dekripsi. Ilmu kriptografi berkembang selaras dengan kemajuan teknologi. Menurut kronologi waktunya ilmu kriptografi dapat dibedakan menjadi dua pemahaman, yakni kriptografi klasik dan kriptografi modern. Kedua pemahaman tersebut bergantung pada penggunaan perangkat analasis dan pembuat pesan yang bersifat kriptologis.

Apa itu kriptografi klasik? Kriptografi klasik adalah kriptografi dalam pembuatannya maupun analisisnya sama sekali tidak melibatkan komputer atau perangkat mesin. Alat-alat yang digunakan berkutat pada pemanfaatan kertas, pena, batu, serta alat-alat lain yang tidak tergolong dalam perangkat mesin modern sama sekali. Ciri khas dari kriptografi klasik ialah lebih berbasis pada karakter, baik karakter tulisan maupun karakter pesan yang disampaikan. Ciri lainnya berupa penggunaan alat-alat yang masih terbilang tradisional karena pada waktu kemunculannya belum mengenal komputer. Itulah cara kerja kriptografi klasik. Semua alogaritma kriptografi (chipper) dari kriptografi klasik termasuk dalam sistem kriptografi yang bersistem simetris. Teknik enkripsi pada kriptografi klasik semuanya sama seperti kunci enkripsi. Maksudnya, untuk memahami sebuah teks tersembunyi dapat dilakukan secara serupa seperti saat pembuatannya.

Kiranya perlu Anda ketahui sebagai basis pemahaman awal kriptografi, yaitu algoritma dalam keilmuan kriptografi. Algoritma sendiri memiliki pengertian sebagai langkah-langkah atau metode yang disusun secara sistematis. Bila ditempelkan pada ‘kriptografi’, maka makna dari algoritma kriptografi adalah langkah logis untuk menyembunyikan pesan. Ada tiga fungsi dasar di dalam algoritma kriptografi, antara lain; enkripsi, dekripsi, dan kunci. Enkripsi berarti proses penyembunyian data pesan, mengubah plaintext menjadi chipertext. Sedangkan dekripsi merupakan kebalikan dari enkripsi, bertujuan untuk memahami pesan yang ada, dan kunci adalah teknik yang digunakan untuk enkripsi maupun dekripsi. Di tataran masa kriptografi modern, kriptografi tidak harus berbentuk besar dan melewati tahapan yang sulit mengerti. Bahkan di era modern, kriptografi sudah dapat dihadirkan secara portable, seperti halnya aplikasi yang menggunakan kriptografi. Aplikasi yang dibuat untuk kriptogrfi berarti sebuah program yang memungkinkan untuk dilakukannya enkripsi dan dekripsi pada saat melakukan proses pengamanan sebuah pesan di dalam data desktop maupun handphone. Aplikasi ini biasanya digunakan untuk mengamankan perangkat maupun isi di dalam perangkat itu sendiri dengan melakukan penguncian yang menggunakan metode algoritma kriptografi. Praktek semacam ini sangat akrab di kriptografi modern karena sarana dan prasarana yang sudah mendukung secara penuh.

Penggunaan dari aplikasi berkriptograf ini membuat keamanan perangkat menjadi berlapis-lapis. Bagi seseorang yang berniat membuka perangkat tersebut, harus melewati beberapa rangkaian kunci yang telah disediakan untuk mengamankan perangkat. Seseorang yang memanfaatkan kriptografi di dalam aplikasi jelas memikili tingkat privasi yang sangat tinggi. Demi kerahasiaan atas privasinya, aplikasi yang menggunakan kriptografi dipandang penting untuk digunakan. Adanya lapisan keamanan yang bertingkat akan membuat orang yang berniat buruk kehabisan kesabaran ketika membongkar. Terdapat banyak sekali aplikasi yang menyediakan layanan kriptografi, malah dalam kenyataannya, setiap aplikasi sudah dilengkapi dengan perangkat kriptografi, contohnya adalah aplikasi WhatsApp dan Telegram. Keduanya mengamankan pengguna melalui kunci enkripsi yang cukup rumit dan ketat demi keterjagaan privasi penggunanya.

1. **Rumusan Masalah**
2. Jelaskan Level Keamanan Sistem dan cakupannya!
3. Terdapat beberapa gangguan dan ancaman sistem informasi baik fisik maupun non fisik. Jelaskan hal tersebut ?
4. Ada beberapa model Kriptografi dan Enkripsi, berikan uraian dengan lengkap dan jelas serta pada review tambahkan contoh simulasi pembuatan chiper text untuk nama kalian dari salah satu model tersebut!

**BAB II**

**PEMBAHASAN**

1. Keamanan level 0 : physical security, merupakan keamanan tahap awal dari keamanan komputer. Keamanan fisik hanya fokus pada fisik saja seperti kunci pintu, cctv, kartu identitas dan sebagainya. Apabila keamanan fisik ini tidak terjaga dengan baik, maka data atau bahkan hardware komputer tidak bisa diamankan.

Keamanan level 1 : terdiri dari keamanan database, keamanan data, keamanan komputer, keamanan perangkat, keamanan aplikasi. Hanya orang-orang yang mempunya wewenang yang dapat mengakses semua keamanan yang disebutkan tadi. Contohnya seperti admin sebuah komputer yang menyimpan berbagai data dan informasi.

Keamanan level 2 : network security, komputer yang terhubung dengan jaringan seperti LAN, WAN ataupun internet sangat rawan dalam masalah keamanan dikarenakan komputer dapat diakses oleh komputer client, oleh karena itu keamanan level 2 harus dirancang supaya tidak terjadi kebocoran jaringan, akses ilegal yang dapat merusak keamanan data tersebut. Maka dari itu, setelah selesai pengerjaan keamanan level 1, maka keamanan level 2 dirancang supaya tidak ada hal-hal yang tidak diinginkan terjadi seperti kebocoran jaringan, illegal access, dan perbuatan illegal lainnya.

Keamanan level 3 : information security, keamanan yang terkadang disepelekan oleh admin seperti meninggalkan password di kertas atau memberikan password kepada teman, makan bisa menjadi suatu hal yang sangat fatal karena dapat disalahgunakan.

Keamanan level 4 : merupakan keamanan yang mencakup keseluruhan dari sistem komputer. Apabila level 1-3 sudah dijalankan dengan baik maka level 4 sudah terpenuhi. Namun tidak menutup kemungkinan bila ada hal-hal illegal dapat terjadi seperti adanya penyusup atau perusakan data dll.

1. Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.

Kejahatan dengan memasukkan data atau berupa informasi ke jaringan internet tentang sesuatu yang tidak benar dan melanggar ketentuan hukum. Contohnya pemuatan berita atau informasi yang tidak benar seperti memuat video pornografi, memuat informasi yang sangat rahasia seperti rahasi negara, dll Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada dokumen melalu internet.

Kejahatan dengan memanfaatkan jaringan internet untuk melakukan mata-mata terhadap pihak yang menjadi sasaran, dengan memasuki sistem jaringan komputer pihak yang menjadi sasarannya.

Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau pengahncuran terhadap data atau sistem jaringan komputer. Misalnya menyusupkan virus komputer dimana data yang terkena virus tidak dapat digunakan lagi.

Kejahatan yang ditujuakan terhadap kekayaan intelektual yang dimiliki pihak lain di Internet.

Kejahatan yang ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data seseorang yang tersimpan pada komputer, dimana jika ada yang mengetahui data tersebut maka dapat merugikan korban. Misalnya nomor pin ATM. Pasword, dan lain-lain.

1. Chaesar Chipper Adalah Salah Satu Algorithma Kriptografi yang Juga Cukup Terkenal. Seperti Namanya, Algoritma ini dicetuskan Oleh Julius Caesar. Metode yang digunakan adalah Substitusi, dimana untuk menghasilkan Chipper Teks, Setiap Teks (Plain Teks) akan diganti dengan Teks yang Lain dengan Selisih tertentu yang telah ditentukan. Contohnya Seperti berikut Misalkan Sandinya adalah 3

Plain Teks -> ADELLA

Maka dengan Menggunakan Sandi 3, Chipper Teksnya akan Menjadi Seperti Berikut

Chipper Teks -> DGHOOD

Cara Kerjanya Sederhana. Setiap Huruf dalam Plain Teks Tersebut diganti dengan 3 huruf setelahnya.

Huruf A diganti dengan D karena dalam alfabet, Huruf ke 3 Setelah A adalah D Begitu Juga dengan Huruf D, E, L, L, dan A masing-masing akan diganti dengan huruf ke 3 Setelahnya.

**BAB III**

**PENUTUP**

**DAFTAR PUSTAKA**

<https://fti.uajy.ac.id/sentika/publikasi/makalah/2015/9.pdf>

<http://student.blog.dinus.ac.id/mkdeffa/2017/10/15/metodologi-keamanan-sistem-informasi/>

<https://www.kompasiana.com/retnowitaningtyas/574bf7dc907a61d906430ca4/beberapa-ancaman-dan-cara-penanggulangan-ancaman-pada-sistem-informasi>

<https://canthafamily.blogspot.com/2014/06/algoritma-chaesar-chiper-dengan-php.html>