BAB II

TINJAUAN PUSTAKA

2.1. Teori Dasar

Pada teori dasar ini, penulis menjelaskan teori tentang jaringan secara umum. Teori yang dijelaskan antara lain jaringan komputer, standar jaringan komputer, jenis jaringan komputer, dan model *OSI Layer.*

a. Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan dari komputer, *printer*, dan peralatan lainnya yang terhubung dalam satu kesatuan dan membentuk suatu sistem tertentu. (Maslan,Andi dan Wangdra,Tonny, 2012). Jaringan computer dapat dibangun dengan menggabungkan antara *hardware* dan *software*. Dua buah komputer yang memiliki sebuah kartu jaringan berbeda, kemudian dikoneksikan dengan maupun tanpa kabel (*nirkabel*) sebagai media untuk mentransmisi data, dan terdapat *software* sistem operasi jaringan yang akan membentuk sebuah jaringan yang sederhana. Tidak semua jaringan komputer sama. Jaringan yang penulis gunakan untuk menghubungkan laptop ini ke router nirkabel, printer, dan peralatan lain adalah yang terkecil yang bisa dibayangkan. Jika bekerja di kantor, jaringan tersebut menggunakan *LAN (Local Area Network)*, biasanya merupakan beberapa komputer terpisah yang terhubung ke satu atau dua *printer, scaner*, dan satu koneksi ke Internet. Jaringan bisa lebih besar dari ini. Di sisi lain ada juga *MAN (Metropolitan Area Network),* yang mencakup seluruh kota, dan *WAN (Wide Area Network)*, yang dapat mencakup area geografis mana pun. Internet adalah *WAN* yang mencakup seluruh dunia.

b. Standar Jaringan Komputer

Standar jaringan komputer tidak dimiliki oleh satu perusahaan telah menjadi keuntungan besar bagi pelanggan produk komputer dan jaringan, serta produsen yang menjualnya. Namun, untuk memfasilitasi pengembangan standar terbuka, diperlukan organisasi yang akan mengoordinasikan pembuatan dan penerbitan dokumen-dokumen ini. Berikut adalah beberapa jenis organisasi standar yang terdapat pada jaringan computer.

1. *ISO (International Organization for Standardization)* Mungkin organisasi standar terbesar di dunia, *ISO* sebenarnya adalah federasi organisasi standar dari banyak negara. Dalam dunia jaringan, *ISO* paling dikenal dengan Model Referensi *OSI*-nya.
2. *American National Standards Institute (ANSI)*: *ANSI* adalah organisasi utama yang bertanggung jawab untuk mengkoordinasikan dan menerbitkan standar komputer dan teknologi informasi di Amerika Serikat. Meskipun umumnya dianggap mengembangkan dan memelihara standar, *ANSI* tidak melakukan keduanya. Sebaliknya, *ANSI* mengawasi dan mengakreditasi organisasi yang benar-benar membuat standar, mengkualifikasinya sebagai *Standards Developing Organiz*ations atau *SDO*. *ANSI* juga menerbitkan dokumen standar yang dibuat oleh *SDO*, dan berfungsi sebagai perwakilan Amerika Serikat untuk *ISO.*
3. *NCITS (National Committee for Information Technology*) Sebuah komite yang dibentuk oleh *ITIC* untuk mengembangkan dan memelihara

standar yang terkait dengan dunia teknologi informasi. NCITS sebelumnya dikenal dengan nama Komite Standar Terakreditasi X3, Teknologi Informasi, atau yang lebih umum hanya X3. Ia memiliki beberapa sub-komite yang mengembangkan dan memelihara standar untuk berbagai mata pelajaran teknis.

4. *IEEE* (*Institute of Electrical and Electronics Engineers)* adalah organisasi profesional terkenal yang bergerak di bidang listrik atau elektronik, termasuk komputer dan jaringan. Klaim utama *IEEE* untuk ketenaran dalam industri jaringan adalah Proyek *IEEE 802*, yang mencakup banyak teknologi jaringan populer termasuk *Ethernet*. (Maslan,Andi dan Wangdra,Tonny, 2012).

c. Model *OSI Layer*

(Sugiyono, 2016) Suatu badan multinasional yang didirikan tahun 1947 yaitu *International Standards Organization (ISO)* merupakan badan yang melahirkan standar-standar internasional. *ISO* ini juga telah mengeluarkan standar dalam bidang jaringan komunikasi yang mencakup segala aspek yaitu model *OSI (Open System Interconnection)*. Tujuan dari *OSI* ini sendiri yaitu memfasilitasi bagaimana suatu komunikasi dapat terjalin dari sistem yang berbeda tanpa memerlukan perubahan yang signifikan pada *hardware* dan *software* ditingkat *under lying*. *OSI Layer* dibagi dalam 7 Lapis (*Layer*), *application, presentation, session, transport, network, data link*, dan *physical. Application Layer* memiliki fungsi untuk pertukaran informasi

antara program komputer, seperti program *e-mail*, dan *service* lain yang jalan dijaringan. Contoh- contoh protokol dalam lapisan ini adalah *HTTP, FTP, SMTP* dan sebagainya. *Presentation Layer* bertanggung jawab atas bagaimana data tersebut akan dikonversi dan diformat untuk transfer data. Konversi format tersebut contohnya *text ASCII* untuk dokumen, *gif* dan *JPG* untuk gambar. *Session Layer* Menentukan bagaimana dua terminal menjaga, memelihara dan mengatur sebuah koneksi, bagaimana mereka akan saling berhubungan, berfungsi untuk mendefinisikan bagaimana suatu koneksi dapat dibuat, dipelihara, maupun dihancurkan. *Transport Layer* memiliki tugas untuk membagi data menjadi segmen, menjaga koneksi logika "*end-to-end*" antar terminal, dan menyediakan penanganan keadaan error (*error handling*). Fungsinya antara lain untuk memcah data ke dalam bentuk paket-paket data serta memberikan nomor urut ke paket-paket tersebut supaya dapat disusun kembali pada sisi tujuan setelah diterima. *Network Layer* memiliki tugaas antara lain untuk menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, dan menjaga antrian trafik di dalam jaringan. Data pada *layer* ini memiliki bentuk paket. Berfungsi mendefinisikan alamat-alamat *IP*, membuat *header* untuk paket-paket, dan setelahnya melakukan *routing* melalui *internetworking* dengan menggunakan *router* serta *switch*. *Data Link Layer* memiliki tugas *link* untuk suatu data, memaketkannya menjadi *frame* yang berhubungan dengan *hardware* kemudian diangkut melalui sebuah media. Komunikasinya dengan kartu jaringan, mengatur komunikasi *layer physical* antara sistem

koneksi serta menangani keadaan atau kondisi *error*, berfungsi juga sebagai bit-bit data dikelompokkan menjadi format yang kita kenal sebagai *frame*. Selain itu, pada level ini akan terjadi pengoreksian pada kesalahan, *flow control*, *Media Acces Control (MAC),* dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub, bridge, repeater, switch layer* 2 bisa beroperasi. Spesifikas *IEEE 802*, membagi level ini menjadi 2 level, yaitu lapisan *Logical Link Control (LLC)* dan lapisan *Media Acces Control (MAC). Physical Layer* bertugas untuk memproses data dan menjadikannya bitlalu mentransfernya melalui media, seperti kabel, dan menjaga koneksi fisik antar system yang ada. Lapisan *physical* ini menentukan spesifikasi koneksi fisik dari jaringan computer itu sendiri. Fungsinya aadalah mendefinisikan media transmisi jaringan, metode untuk pensinyalan, sinkronisasi bit, arsitektur jaringan seperti topologi jaringan dan pengkabelan. Pada level ini juga bisa mendefinisikan bagaimana *Network Interface Card (NIC)* dapat melakukan interaksi dengan media kabel atau radio.

2.2. Teori Khusus

Pada teori khusus penulis membahas tentang keamanan jaringan, serangan keamanan jaringan, *file*, format, kriptografi, dan *vigenere cipher.*

a. Keamanan Jaringan

Keamanan jaringan menjadi lebih penting bagi pengguna komputer pribadi, organisasi, dan militer. Dengan munculnya internet, keamanan menjadi perhatian

utama dan memungkinkan keamanan menjadi lebih baik dengan pemahaman tentang munculnya teknologi keamanan. (Funmilola dan Oluwafemi, 2015). Setiap organisasi, terlepas dari ukuran, industri, atau infrastruktur, membutuhkan tingkat solusi keamanan jaringan untuk melindungi dari ancaman *hacker* yang terus tumbuh di dunia saat ini.

Arsitektur jaringan saat ini sangat kompleks dan dihadapkan dengan lingkungan ancaman yang selalu berubah dan penyerang yang selalu berusaha menemukan dan mengeksploitasi kerentanan. Kerentanan ini terdapat di sejumlah area, termasuk perangkat, data, aplikasi, pengguna, dan lokasi. Karena alasan ini, ada banyak alat dan aplikasi manajemen keamanan jaringan yang digunakan saat ini yang membahas ancaman dan eksploitasi individu dan juga ketidakpatuhan pada peraturan. Ketika hanya beberapa menit server *down* dapat menyebabkan gangguan yang meluas dan kerusakan besar pada *file* dan reputasi organisasi atau perusahhan, sangat penting bahwa langkah-langkah perlindungan ini ada.

1. Cara Kerja Keamanan Jaringan

Ada banyak lapisan yang perlu diperhatikan saat menangani keamanan jaringan di dalam organisasi. Karena serangan dapat terjadi baik di perangkat keras maupun perangkat lunak itu sendiri maka keamanan pada setiap area harus sangat diperhatikan.

b. Jenis-jenis Umum dari Serangan Keamanan Jaringan

1. Serangan *Phishing*

Definisi *phising* adalah kegiatan dari seseorang atau lebih untuk memperoleh informasi atau data rahasia pengguna dalam suatu situs dengan menggunakan *email* dan situs palsu yang memiliki tampilan yang mirip dengan tampilan dari situs yang asli atau resmi. (Rachmawati, 2014). Itu terjadi ketika seorang penyerang menyamar sebagai individu terpercaya, menipu korban untuk membuka pesan teks, email, atau pesan instan. Korban kemudian ditipu untuk membuka tautan jahat yang dapat menyebabkan pembekuan sistem sebagai bagian dari serangan *ransomware*, mengungkapkan informasi sensitif, atau pemasangan *malware*.

Bagi seorang individu, ini termasuk pencurian identitas, pencurian uang, atau pembelian tanpa izin. Phishing sering digunakan untuk mendapatkan celah di jaringan pemerintah atau perusahaan sebagai bagian dari plot yang lebih signifikan seperti *advanced persistent threat (APT).* Dalam kasus seperti itu, karyawan dikompromikan untuk mendapatkan akses istimewa ke data aman, mendistribusikan *malware* di lingkungan tertutup, dan memintas parameter keamanan.

2. Serangan *Spear Phishing*

Spear phishing adalah *email* yang ditargetkan pada individu atau grup tertentu, bukan mengirim spam ke pengguna acak. *Spear phishing* biasanya diawali dengan perencanaan yang matang ke calon korbannya. Penyerang kemudian dapat mengirim pesan yang tampak seperti asli dari sumber yang terpercaya. (Sagar, Shivani, & Chakravarty, 2019). Peretasan ini tidak dilakukan

oleh penyerang acak tetapi kemungkinan besar dilakukan oleh orang-orang yang keluar karena rahasia dagang, keuntungan finansial, atau intelijen militer.

Email spear phishing tampaknya berasal dari seseorang di dalam organisasi penerima sendiri atau seseorang yang dikenal secara pribadi oleh target. Cukup sering peretas yang disponsori pemerintah melakukan kegiatan ini. Penjahat dunia maya juga melakukan serangan ini dengan tujuan menjual kembali data rahasia ke perusahaan swasta dan pemerintah. Penyerang ini menggunakan rekayasa sosial dan pendekatan yang dirancang secara individual untuk mempersonalisasi situs web dan pesan secara efektif.

3. Serangan *Malware*

Malware sendiri merupakan kata atau istilah umum yang digunakan untuk mewakili berbagai bentuk perangkat lunak berbahaya, Perangkat lunak apa pun sengaja didesain untuk niat buruk bisa dikategorikan sebagai *malware*. (D, Vijayanand C S, dan Arunlal K, 2019). Definisi luas ini mencakup banyak jenis perangkat lunak jahat *(malware)* tertentu seperti *spyware*, *ransomware*, perintah, dan kontrol. Banyak pelaku bisnis dan pelaku kriminal yang terkenal telah terlibat dan menemukan penyebaran *malware*. *Malware* berbeda dari perangkat lunak lain karena dapat menyebar ke seluruh jaringan, menyebabkan perubahan dan kerusakan, tetap tidak terdeteksi, dan gigih dalam sistem yang terinfeksi. Itu dapat menghancurkan jaringan dan membuat kinerja mesin bertekuk lutut. Dalam sebuah bisnis, administrator keamanan sistem dapat mengurangi efektivitas

peretasan seperti itu dengan mendorong staf manajemen perusahaan untuk menghadiri pelatihan kesadaran keamanan.

4. *Trojan Horse*

Trojan horse adalah program berbahaya yang dapat merepresentasikan dirinya dengan menyamar sebagai program biasa, program ini digunakan untuk mengelabui korbannya. (Okereke & Chukwunonso, 2018). *Trojan horse* biasanya membawa fungsi tersembunyi yang diaktifkan saat aplikasi dimulai. . Mereka menyebar dengan terlihat seperti perangkat lunak rutin dan membujuk korban untuk menginstal. *Trojan horse* dianggap sebagai salah satu jenis *malware* yang paling berbahaya, karena sering dirancang untuk mencuri informasi keuangan.

5. Serangan *Distributed Denial-of-Service (DDoS)*

Distributed Denial-of-service (DDoS) adalah upaya untuk menghabiskan *bandwidth* korban atau mengganggu akses pengguna ke layanan internet. (Prasad, Reddy, & Rao, 2014). Serangan ini mempunyai misi yaitu dengan membanjiri target dengan *bandwidth* atau membanjirinya dengan informasi yang memicu kerusakan. Dalam kedua situasi tersebut, serangan *DDoS* menyangkal pengguna yang sah seperti karyawan, pemegang akun, dan anggota sumber daya atau layanan yang mereka harapkan.

Serangan *DDoS* sering ditargetkan pada server web organisasi profil tinggi seperti organisasi perdagangan dan pemerintah, perusahaan media, perdagangan, dan perbankan. Meskipun serangan-serangan ini tidak mengakibatkan hilangnya atau pencurian informasi penting atau aset lainnya, mereka dapat menghabiskan

banyak uang dan waktu bagi korban untuk menginvestigasi. *DDoS* sering digunakan dalam kombinasi untuk mengalihkan perhatian dari serangan jaringan lainnya.

c. *File*

Sederhananya, *file* adalah wadah yang menyimpan jenis informasi tertentu, seperti *file* gambar, lagu, atau dokumen. (Moran, 2015). Di Windows, setiap *file* memiliki nama dan ekstensi (ekstensi biasanya terdiri dari tiga karakter, tetapi bisa jadi dua atau empat) misalnya, anggaran keluarga.xlsx. Ekstensi *file* memberi tahu jenis informasi yang dikandung *file* sehingga program akan membukanya. Contohnya, ekstensi xlsx menunjukkan bahwa *file* dapat dibuka dengan menggunakan Microsoft Excel atau program lain yang kompatibel. Data-data yang berasal dari dokumen atau *file* pengolah kata, angka-angka untuk perhitungan, nama maupun alamat dalam basis suatu data adalah contoh masukan data teks yang terbentuk dari karakter, angka serta tanda baca. Kemudian bentuk masukan serta keluaran dari data teks direpresentasikan menjadi set karakter atau sistem kode yang dapat dikenali oleh sistem komputer. Set karakter yang digunakan untuk masukan dan keluaran data umunya ada tiga, yaitu *ASCII*, *EBCDIC,* dan *Unicode*.

1. Format *(*.txt)*

Format **.txt* adalah format teks yang berguna untuk menyipan data berbentuk huruf, angka, karakter control atau simbol-simbol yang biasanya digunakan dalam penulisan santara lain tanda tanya, koma, tanda petik, titik dan

sebagainya. Satu huruf, angka, karakter kontrol atau simbol pada arsip teks biasanya memakan tempat satu *byte*. sedangkan jenis teks terformat yang satu huruf saja dapat memakan tempat beberapa *byte* untuk menyimpan format dari huruf tersebut seperti font, ukuran, tebal atau tidak dan lainnya. Kelebihan dari format **.txt* ini yaitu ukuran datanya yang lebih kecil karena tidak terdapat fitur untuk memformat tampilan dari teks itu sendiri. Perangkat lunak pada masa ini yang paling banyak digunakan oleh masyarakat untuk memanipulasi bentuk format data ini adalah *Notepad*.

Gambar 2.1 *File *.txt*
Sumber : (Data penelitian 2021)

2. Format *(*.doc)*

Format ***.**doc* adalah ekstensi dari arsip dokumen perangkat lunak *microsoft word* yang paling banyak digunakan untuk menulis bentuk laporan, makalah dan sebagainya. ***.**doc* merupakan jenis teks terformat yang dapat mengatur tampilan teks seperti *styles* (*font*, ukuran huruf, dan sebagainya), dan juga dapat menyisipkan gambar kealamnya. Kekurangan dari format ***.**doc* ini sendiri ada pada ukuran datanya yang cukup besar disbanding format lain.

Gambar 2.2 *File *.doc*
Sumber : (Data penelitian 2021)

3. Format *(*.xls)*

Format ***.xls** adalah ekstensi arsip dokumen pada perangkat lunak *Microsoft excel* yang paling banyak digunakan dan cukup popular dalam pembuatan lembar kerja *spreadsheet* karena dilengkapi berbagai fitur kalkulasi akurat dan mudah dijalankan. Sampai saat inipun *microsoft excel* adalah salah satu program *spreadsheet* terpopuler dan dipergunakan oleh berbagai macam kalangan, baik di *platform Windows* maupun *Mac OS*.

Dalam mengoprasikan format inipun cukup gampang, apalagi jika kita sudah mengetahui rumus - rumus dan logika perhitungan pada *excel*, maka menggunakan aplikasi ini pun tidak akan sulit. Dan juga sebaliknya, apabila kita belum paham rumus dan logika perhitungannya maka untuk menjalankan format inipun akan terasa sulit, karena kesalahan dalam menggunakan rumus dapat mengakibatkan terjadinya kesalahan dalam membaca hasil data. Karena itu kita sangat perlu mempelajari rumus dan logika *excel* dengan benar dan baik agar dapat menggunakan format *excel* dengan benar.

Gambar 2.3 *File *,xls*
Sumber : (Data penelitian 2021)

4. Format *(*.pdf)*

Format **.pdf* merupakan jenis format data dalam bentuk dokumen atau berkas yang pertukarannya dilakukan secara digital, format ini dibuat oleh *Adobe System* pada tahun 1993. Pada awalnya format ini digunakan untuk kepentingan pertukaran dokumen secara digital, namun pada saat ini format **.pdf* ini juga sering digunakan untuk presentasi dokumen dua dimensi yang terdiri dari *text*, huruf, *vector* grafik serta citra. Adobe System Inc kini juga mengembangkan program *Acrobat 3-D* yang membuat *PDF* mampu untuk membaca dokumen dalam bentuk tiga dimensi. Saat ini *PDF* sendiri sudah menjadi standar *ISO* dengan kode 32000-1:2008 sejak Juli 2008.

Format **.pdf* ini juga sangat sering dipergunakan dalam administrasi perkantoran karena kemudahan penggunaan serta kemampuannya. Pada awalnya format ini tidak terlalu diminati karena kalah saing dengan pendahulunya yaitu *Microsoft office*, namun karena kemampuannya yang makin berkembang dan mudah digunakan maka saat ini format *PDF* juga banyak digunakan oleh khalayak ramai.

Gambar 2.4 *File *.pdf*
Sumber : (Data penelitian 2021)

d. Kriptografi

Kriptografi yaitu bentuk ilmu yang digunakan untuk mempelajari cara untuk menjaga agar data atau pesan tetap dalam kondisi aman saat dikirimkan, dari pengirim ke penerima tanpa diganggu oleh pihak lain. Konsep kriptografi ini sebenarnya telah lama digunakan oleh manusia pada peradaban Mesir dan Romawi walaupun metodernya masih sangat sederhana tidak seperti sekarang ini. Prinsip-prinsip yang menjadi dasar dari kriptografi antara lain: *Confidentiality* (kerahasiaan) yang merupakan layanan agar data atau pesan yang dikirim dari seseorang tetap terjaga kerahasiaannya sampai ditangan si penerima tanpa gangguan kecuali mendapat izin dari pihak yang terkait. Cara yang umum dilakukan adalah dengan membuat alogaritma otomatis yang mampu mengubah data yang dikirim menjadi sulit untuk dibaca atau dipahami. Data *integrity* (keutuhan data) adalah kemampuan untuk mengetahui adanya manipulasi data dari pihak lain yang tidak terkait. *Authentication* (otentikasi) adalah layanan untuk mengidentifikasi otentikasi keaslian data/informasi tersebut. *Nonrepudiation* (anti-penyangkalan) yaitu layanan untuk mencegah suatu pihak untuk menyangkal

aksi yang telah dilakukan sebelumnya atau menyangkal bahwa pesan tersebut berasal dirinya.

Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:

1. *Plaintext*, adalah pesan yang dapat dibaca
2. *Ciphertext*, adalah pesan acak yang tidak dapat dibaca
3. *Key*, adalah kunci untuk melakukan teknik kriptografi
4. *Algorithm*, adalah metode untuk melakukan enkrispi dan dekripsi

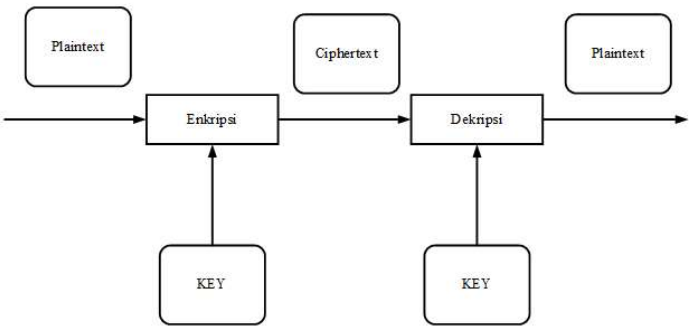
Adapun proses dasar pada Kriptografi yaitu:

1. Enkripsi (*Encryption*)

Enkripsi merupakan metode atau cara yang digunakan untuk mengubah informasi menjadi kode rahasia yang menyembunyikan makna sebenarnya dari informasi tersebut. Ilmu mengenkripsi dan mendekripsi informasi disebut kriptografi.

2. Dekripsi (*Decryption*)

Dekripsi adalah proses mengambil teks yang disandikan atau dienkripsi atau data lain dan mengubahnya kembali menjadi teks yang dapat di baca dan pahami oleh komputer. Umumnya merupakan lawan dari enkripsi. Ini menerjemahkan informasi terenkripsi sehingga pengguna yang berwenang yang hanya dapat mendekripsi data karena dekripsi memerlukan kunci rahasia atau kata sandi.



Gambar 2.5 Enkripsi dan Dekripsi
Sumber : (Data penelitian 2021)

e. *Vigenere cipher*

Vigenere Cipher adalah *cipher* blok polialfabetik, tetapi jika dilihat dengan cara lain, ini adalah *stream cipher* yang merupakan generalisasi alami dari sandi geser (Smart, 2013). *Vigenere Cipher* adalah suatu bentuk pengembangan dari *caesar cipher*. Kelebihan dari sandi ini dibandingkan *Caesar Cipher* dan *cipher* polialfabetik lainnya adalah *cipher* ini tidak begitu rentan terhadap metode pemecahan *cipher* yang disebut analisis frekuensi. *Cipher* ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. *Vigenere Cipher* adalah metode mengenkripsi teks alfabet dengan menggunakan huruf/tabel dan angka. Tabel ini biasanya disebut sebagai *Vigenere Table*, *Vigenere Table atau Vigenere Square*. Penulis akan menggunakan Tabel *Vigenere*. Baris pertama tabel ini memiliki 26 huruf alfabet. Dimulai dengan baris kedua, setiap baris memiliki huruf bergeser ke posisi satu kiri. Misalnya, ketika B digeser ke posisi pertama di baris kedua, huruf A bergerak ke akhir.

Tabel 1.1 Tabel *Vigenere*

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

Sumber : (Data penelitian 2021)

Contoh:

PLAINTEXT : EDI SUSANTO

KEY : EDIEDIEDIE

CIPHERTEXT: IGQWXAEQBS

Perhitungan kriptografi *vigenere cipher* :

Enkripsi

$$Ci = (Pi + Ki) \bmod 26$$

Jika hasil P+K sama atau lebih dari 26 maka hasil dari P+K dikurang 26

Dekripsi

$$Pi = (Ci - Ki) \bmod 26$$

Dimana

C_i = Nilai desimal karakter *ciphertext* ke-i

P_i = Nilai desimal karakter *plaintext* ke-i

K_i = Nilai desimal karakter kunci ke-i

26 = Panjang abjad dari A-Z

Nilai desimal karakter:

A=0 B=1 C=2 … Z=25

Contoh:

PLAINTEXT : EDI SUSANTO

KEY : EDIEDIEDIE

CIPHERTEXT : IGQWXAEQBS

$C_I = (P_i + K_i) \bmod 26$ P=E

$= (4 + 4) \bmod 26$ K=E

$= 8 \bmod 26$

$= 8$ (H)

$C_I = (P_i + K_i) \bmod 26$ P=D

$= (3 + 3) \bmod 26$ K=D

$= 6 \bmod 26$

$= 6$ (G)

$C_I = (P_i + K_i) \bmod 26$ P=I

$= (8 + 8) \bmod 26$ K=I

$= 16 \bmod 26$

$= 16$ (Q)

$C_I = (P_i + K_i) \bmod 26$ P=S

$= (18 + 4) \bmod 26$ K=E

$= 22 \bmod 26$

$= 22$ (W)

$C_I = (P_i + K_i) \bmod 26$ P=U

$= (20 + 3) \bmod 26$ K=D

$= 23 \bmod 26$

$= 23$ (X)

$C_I = (P_i + K_i) \bmod 26$ P=S

$= (18 + 8) \bmod 26$ K=I

= 26 mod 26

= 0 (A)

$C_I = (P_i + K_i) \bmod 26$ P=A

= (0 + 4) mod 26 K=E

= 4 mod 26

= 4 (E)

$C_I = (P_i + K_i) \bmod 26$ P=N

= (13 + 3) mod 26 K=D

= 16 mod 26

= 16 (Q)

$C_I = (P_i + K_i) \bmod 26$ P=T

= (19 + 8) mod 26 K=I

= 27 mod 26

= 1 (B)

$C_I = (P_i + K_i) \bmod 26$ P=O

= (14 + 4) mod 26 K=E

= 18 mod 26

= 18 (S)

2.3. *Software* Pendukung

Berikut ini adalah *software* yang digunakan dalam penelitin ini yaitu:

2.3.1 IntellijIdea

IntellijIdea adalah *IDE*, atau *Integrated Development Environment*, yang dibuat oleh JetBrains. IntelijIdea mengintegrasikan semua alat pengembangan yang mungkin diperlukan ke dalam satu tempat. Versi pertama IntellijIdea dirilis pada Januari 2001. IntellijIdea adalah *IDE* java pertama yang memiliki kemampuan navigasi kode dan refactor kode tingkat lanjut. Pada tahun 2010, ia terpilih sebagai alat pemrograman terbaik yang tersedia untuk java.

Gambar 2.6 *Software* IntellijIdea
Sumber : (Data penelitian 2021)

2.4. Penelitian Terdahulu

Pada penelitian terdahulu penulis akan merangkum atau menyimpulkan beberapa jurnal yang berhubungan dengan judul skripsi. Beberapa diantaranya adalah :

1. Aplikasi Kriptografi Pesan Menggunakan Algoritma *Vigenere Cipher*

Menurut (Efrandi dan kawan kawan, 2014 ISSN : 1858 - 2680) dalam Jurnal yang berjudul "APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA *VIGENERE CIPHER*", cara ataumetode yang digunakan adalah algoritma kriptografi *vigenere cipher*. Terdapat kesimpulan bahwa untuk merancang aplikasi kripto dalam sistem ini dilalui dalam beberapa tahap yaitu perancangan diagram, *flowchart*, tampilan program, dan pengkodean algoritma *Vigenere cipher* diimplementasikan pada visual basic 6.0. Program aplikasi kripto sistem ini dapat menyembunyikan pesan penting yang bisa dibaca menjadi tidak bisa dibaca dan mencari maksud dari pesan yang rahasia menjadi bisa dibaca.

2. Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher*

Menurut (Yulianingsih & Maharani, 2014 ISSN 1858-4853) dalam jurnalnya yang berjudul "APLIKASI *CHATTING* RAHASIA MENGGUNAKAN ALGORITMA *VIGENERE CIPHER*" dapat disimpulkan bahwa kriptografi ini merupakan teknik yang bisa digunakan untuk melakukan pengamanan terhadap berbagai tipe *file*, salah satunya berupa pesan teks. Metode *Vigenere Cipher* merupakan suatu metode atau cara yang digunakan dalam perhitungan yang mudah untuk diterapkan dalam penyandian pesan teks baik berupa angka, huruf, bahkan simbol. Sehingga dengan menggunakan metode *Vigenere Cipher* maka dapat dilakukan percakapan yang bersifat rahasia dengan pada aplikasi *chatting*. Aplikasi *chatting* rahasia ini dapat diimplementasikan pada jaringan *LAN*.

3. Implementasi Kriptografi Dengan Enkripsi *Shift Vigenere Chiper* Serta *Checksum* Menggunakan *CRC32* Pada Data *Text*

Menurut (Anwar, Nugroho, & Ahmadi, 2015 ISSN: 2406-7768) dalam jurnalnya yang berjudul **"**IMPLEMENTASI KRIPTOGRAFI DENGAN ENKRIPSI *SHIFT VIGENERE CHIPER* SERTA *CHECKSUM* MENGGUNAKAN CRC32 PADA DATA *TEXT*", metode yang digunakan adalah *shift vigenere chiper* serta *checksum* menggunakan *crc32* mengungkapkan bahwa berhasil dikembangkannya program aplikasi kriptografi untuk pengamanan baik pesan maupun *file*. Kebutuhan fungsional dari program aplikasi, seperti proses enkripsi dan *error checking*. Program ini telah berhasil menyisipkan dan mengekstrasi pesan rahasia dengan sempurna, karena pada hasilnya pesan yang diekstraksi sama dengan pesan yang disisipkan, serta tidak merubah sedikitpun *text* dalam text tersebut. Serta penggunaan kunci *(key)* sudah dilakukan dengan tepat.

4. Algoritma *Vigenere Cipher* Dan *Hill Cipher* Dalam Aplikasi Keamanan Data Pada *File* Dokumen

Menurut (Manaor, Pardede, Manurung, & Filina, 2017 ISSN : 2548-9704) dalam jurnalnya yang berjudul "ALGORITMA *VIGENERE CIPHER* DAN *HILL CIPHER* DALAM APLIKASI KEAMANAN DATA PADA *FILE* DOKUMEN", metode yang diterapkan yaitu algoritma *vigenere cipher* dan *hill cipher*. Mengungkapkan bahwa Sistem ini menggunakan Algoritma *Vigenere Cipher* dan algoritma *Hill Cipher*, kunci dari algoritma *Hill Cipher* menggunakan matriks berordo 2x2 dan kunci matriks tersebut telah ditetapkan oleh sistem, sehingga untuk pengembangan selanjutnya dapat mengenkripsi dan dekripsi dengan *user*

yang menginputkan matriks serta menggunakan matriks berordo 3x3, 4x4, sampai dengan nxn.

5. Efektivitas Pesan Teks dengan *Cipher* Substitusi, *Vigenere Cipher*, dan *Cipher* Transposisi

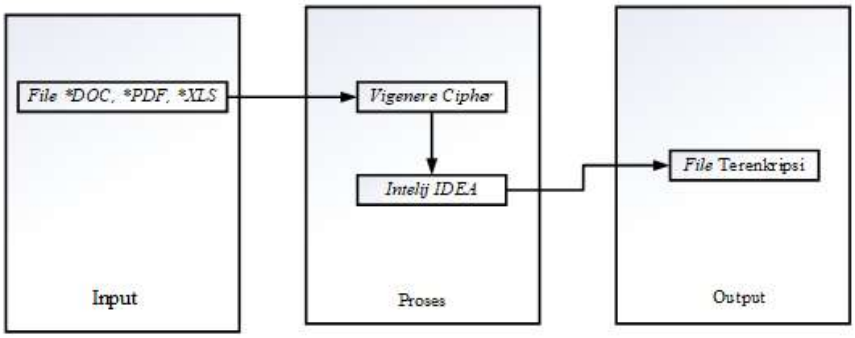
Menurut (Maricar dan Sastra, 2018 p-ISSN:1693 – 2951; e-ISSN: 2503-2372) dalam jurnalnya yang berjudul "EFEKTIVITAS PESAN TEKS DENGAN *CIPHER* SUBSTITUSI, *VIGENERE CIPHER*, DAN *CIPHER* TRANSPOSISI", metode yang digunakan adalah *cipher* substitusi, *vigenere cipher*, serta *cipher* transposisi. Dapat disimpulkan bahwa dari tujuh kombinasi metode yang diproses, dinyatakan berhasil dilakukan proses enkripsi dan dekripsi. Dalam perbandingan efektivitas, digunakan dua alat ukur, yaitu ukuran *file* dan waktu proses. Berdasarkan ukuran *file*, diperoleh hasil untuk ukuran *file* terbesar dalam bentuk kombinasi metode Substitusi, *vigenere*, dan transposisi dengan ukuran *file* 11 Kb. Sedangkan untuk ukuran *file* terkecil adalah metode Substitusi dan metode *vigenere* dengan ukuran *file* 5 Kb. Berdasarkan waktu prosesnya, didapatkan hasil untuk waktu terlama adalah kombinasi metode substitusi, *vigenere*, dan transposisi dengan waktu 1.54 detik. Sedangkan waktu tercepat adalah metode Substitusi dengan waktu 0.37 detik.

6. Pengamanan *File* Dokumen Menggunakan Kombinasi Metode Subtitusi Dan *Vigenere Cipher*

Menurut (Budi, Purba, & Mulyana, 2019 p-ISSN 2087-1716 e-ISSN 2548-7779) dalam jurnalnya yang berjudul "PENGAMANAN *FILE* DOKUMEN MENGGUNAKAN KOMBINASI METODE SUBTITUSI DAN *VIGENERE CIPHER*", metode yang diterapkan merupakan kombinasi metode subtitusi dan *vigenere cipher*. Kemudian didapatkan kesimpulan bahwa aplikasi kriptografi ini dapat diaplikasikan pada *software database MySQL* menggunakan sistem operasi linux maupun sistem operasi berlisensi sebagai keamanan data *file* dokumen dengan metode kombinasi algoritma substitusi dan *vigenere cipher* ini menghasilkan *file* yang terenkrip atau rahasia dalam format *file* *.*txt* yang secara kualitas dan ukuran sama dari ukuran *file text* awal. Dalam pengembangan aplikasi ini sangat disarankan media kriptografi berupa multimedia seperti keamanan data *file* yang berbentuk gambar dan format *file text* yang bervariasi seperti format *.*odt,* *.*docx* maupun format lainnya. Pesan yang dienkripsi maupun di deskripsi tidak hanya berupa *file text*, dapat dikembangkan dengan pesan suara, gambar atau multimedia lain.

2.5. Kerangka Pemikiran

Secara umum, kerangka pemikiran yang digunakan oleh penulis dapat disusun dalam suatu diagram alir penelitian seperti tercantum dibawah ini. Dalam diagram alir ini menunjukkan tiap tahap-tahap proses penelitian yang dilakukan oleh penulis dari tahap awal sampai tahap akhir dari kegiatan penelitian ini,



Gambar 2.7 Kerangka Pemikiran
Sumber : (Data penelitian 2021)

Pada proses *input file* yang bisa dimasukkan adalah *file* yang berformat **.pdf, *.xls, *.doc, dan *.txt.* Proses selanjutnya *file* dienkripsi menggunakan kriptografi *vigenere cipher*. Pada tahap *output file* akan terenkripsi dengan aman.