BAB II

TINJAUAN PUSTAKA

II.1. Penelitian Terkait

Pada penelitian yang dilakukan oleh Haval I. Hussein & Wafaa M. Abduallah (2021) mengusulkan untuk mengatasi kelemahan yang ada. Modifikasi dilakukan untuk mengurangi ukuran *ciphertext* dan mempercepat waktu eksekusi. Ini dilakukan dengan menggunakan operasi tambahan sebagai ganti pengulangan dalam proses enkripsi. Berdasarkan hasil percobaan yang dilakukan, skema yang diusulkan mengurangi tingkat ekspansi sebesar 89%. Serta mempercepat eksekusi waktu yang membuat skema yang diusulkan berkinerja lebih baik. Jadi, tujuan untuk meningkatkan efisiensi *ElGamal Cryptosystem* meningkat secara signifikan. Keamanan skema yang diusulkan tidak terpengaruh yang sama dengan keamanan yang ada didasarkan pada kesulitan memecahkan diskrit masalah logaritma.

Peneliatian lain yang dilakukan oleh Demba Sow & Mamadou Ghouraissiou Camara (2019) menghasilkan varian baru dari skema tanda tangan ElGamal yang disebut "skema tanda tangan ElGamal Umum" diusulkan pada tahun 2011. Skema tanda tangan ElGamal Umum adalah skema tanda tangan ElGamal yang dimodifikasi. Dalam penelitian ini, diusulkan bukti keamanan skema tanda tangan Generalized ElGamal dalam model oracle acak. Beberapa keamanan gagasan skema tanda tangan dan menunjukkan keamanan skema ElGamal Signature yang dimodifikasi. Kami telah berhasil membuktikan eksogisme skema tanda tangan

Generalized ElGamal yang eksistensial, secara adaptif terhadap serangan pesan yang dipilih, dalam model oracle acak.

Penelitian yang dilakukan oleh Djebaili Karima & Melkemi Lamine (2019) diusulkan versi aman dari cryptosystem kunci publik Elgamal, dan membuktikan bahwa itu aman secara semantik dengan asumsi apa yang kita sebut masalah dua dimensi keputusan Diffie-Hellman (2DDDH), *cryptosystem* ini dibedakan oleh kecepatan proses enkripsi dan dekripsi dan oleh ketahanannya terhadap musuh yang aktif. Karena masalah 2DDDH lebih sulit daripada masalah *Diffie-Hellman (DDH) decisional* (seperti yang akan dilihat), kita dapat menyimpulkan bahwa model tersebut memperkuat keamanan pertukaran dibandingkan dengan *cryptosystems* yang ada yang berada dalam konteks yang sama, juga kami membahas kesulitan masalah yang menjamin keamanannya. Dalam penelitian ini, masalah komputasi baru yang disebut masalah Diffie-Hellman (2DDDH) keputusan dua dimensi. Ekstensi ini dapat digunakan dalam banyak konstruksi kriptografi yang didasarkan pada masalah DL. Selain itu, masalah 2DDDH lebih sulit daripada masalah DDH biasa yang diandalkan oleh beberapa skema berbasis masalah logaritma. Paradigma baru kami memiliki banyak aplikasi. Sebagai salah satu aplikasi tersebut, kami menghadirkan varian baru enkripsi ElGamal dengan bukti keamanan yang sangat sederhana.

Penelitian yang dilakukan oleh Gupta, dkk (2018) menyajikan cryptosystem yang berasal dari versi quantum dari diffie-hellman seperti yang dijelaskan sebelumnya, tetapi mungkin dilihat sebagai perbaikan karena *Cryptosystem Elgamal* dapat digunakan untuk menandatangani pesan atau enkripsi dalam satu

arah tanpa interaksi langsung antara para pihak. Protokol pertukaran pasangan urutan qubit antara dua pihak melalui saluran kuantum dan menggunakan basis komputasi sebagai parameter untuk transformasi rotasi kuantum komutatif untuk mendekripsi pesan. Kriptografi pos kuantum adalah bidang penelitian terbaru yang muncul setelah pengenalan algoritma Shor. Cryptosystems klasik seperti RSA, Diffie-Hellman dan ElGamal akan sepenuhnya usang dengan komputer kuantum.

Peneltian juga dilakukan oleh E.Jincharadze (2018) mennjelaskan kriptografi adalah ilmu atau studi tentang teknik penulisan rahasia, terutama sistem kode dan sandi, metode, dan sejenisnya. Kriptografi harus memastikan keamanan tingkat tinggi dalam mentransfer dan menyimpan data. Ada dua jenis algoritma kriptografi seperti kriptografi kunci simetris dan kriptografi kunci asimetris. Saat ini ada berbagai jenis algoritma kriptografi yang memberikan keamanan informasi yang tinggi, tetapi mereka juga memiliki beberapa kelemahan. Untuk meningkatkan kelemahan dari algoritma ini, dalam makalah ini kami mengusulkan model algoritma kriptografi hybrid baru. Algoritma ini dirancang menggunakan kombinasi dua algoritma kriptografi AES dan Elgamal. Telah dilakukan analisis dan perbandingan kinerja algoritma yang diusulkan dengan mengikuti parameter waktu enkripsi, waktu dekripsi dan persyaratan sistem. Untuk algoritma kriptografi ini dibuat program di Java dalam NetBeans IDE. Implementasi dan analisis kinerja model yang diusulkan ini dilakukan oleh Jawa. Sebagai hasil akhir menunjukkan model hybrid memiliki kinerja yang lebih baik daripada sistem AES dan Elgamal (Jincharadze, 2018).

Penelitan lain yang dilakukan Yuling Luo, dkk (2019) menghasilkan penelitian mengenai masalah keamanan tentang manajemen kunci dan distribusi untuk skema enkripsi gambar simetris, metode enkripsi gambar asimetris baru diusulkan dalam makalah ini, yang didasarkan pada kurva eliptik ElGamal (EC-ElGamal) kriptografi dan teori chaotic. Secara khusus, hash SHA-512 pertama kali diadopsi untuk menghasilkan nilai awal dari sistem yang kacau, dan permutasi persilangan dalam hal urutan indeks kacau digunakan untuk mengacak gambar biasa. Selanjutnya, gambar acak yang dihasilkan disematkan ke dalam kurva eliptik untuk dienkripsi oleh EC-ElGamal yang tidak hanya dapat meningkatkan keamanan tetapi juga dapat membantu memecahkan masalah manajemen kunci. Akhirnya, permainan kekacauan gabungan difusi dengan urutan DNA dijalankan untuk mendapatkan gambar sandi. Analisis eksperimental dan perbandingan kinerja menunjukkan bahwa metode yang diusulkan memiliki keamanan tinggi, efisiensi yang baik, dan ketahanan yang kuat terhadap serangan teks biasa yang dipilih yang membuatnya memiliki aplikasi potensial untuk komunikasi gambar yang aman.

Penelitian lain tentang enkripsi Elgamal juga dilakukan oleh Motilal Singh Khoirom, dkk (2021) melakukan enkripsi menggunakan enkripsi kunci publik Elgamal pada bidang yang terbatas memerlukan penyisipan pesan yang diwakili oleh bilangan bulat. Bilangan bulat ini harus ditanamkan ke lokasi koordinat yang memenuhi persamaan kurva eliptik menggunakan teknik penanaman Koblitz. Dengan demikian, ekspansi data terjadi karena setiap bilangan bulat harus direpresentasikan sebagai koordinat. Kurva eliptik yang direkomendasikan

memiliki nilai prima modulo yang besar, sehingga untuk setiap representasi bilangan bulat kecil dari sebuah pesan, perluasan dalam teks sandi sangat besar. Faktor-faktor di atas menghambat penggunaan metode ElGamal untuk enkripsi ukuran data yang besar. Pada versi ameliorated, setiap koordinat dalam persamaan kurva eliptik dapat digunakan untuk melakukan operasi enkripsi. Teknik penanaman Koblitz yang khas ke koordinat tertentu yang memenuhi persamaan kurva eliptik dapat dihindari. Masalah ekspansi data ditangani dengan menggunakan operasi konversi dasar dengan beberapa data audio. Hasil simulasi dan perbandingan kinerja dengan kriptosistem kunci publik lainnya menandakan bahwa metode yang diusulkan cocok untuk operasi enkripsi audio (Khoirom et al., 2021).

Tabel 2.1. Penelitian Perbandingan Penggunaan Algoritma Elgamal

No	Penulis	Judul	Tahun	Hasil Penelitian
1	Haval I. Hussein dan Wafaa M. Abduallah	An Efficient Elgamal Cryptosystem Scheme	2021	Skema yang diusulkan mengurangi tingkat ekspansi sebesar 89% serta mempercepat eksekusi waktu.
2	Demba Sow dan Mamadou Ghouraissiou Camara	Provable Security of The Generalized Elgamal Signature Scheme	2019	Varian baru dari skema tanda tangan Elgamal yang disebut "skema tanda tangan Elgamal Umum"
3	Gupta dan Biswas	Design of lattice-based Elgamal encryption and signature schemes using SIS problem	2018	Cyptosystem yang berasal dari versi quantum dari diffiehellman sebagai perbaikan Cryptosystem Elgamal yang digunakan untuk menandatangani pesan satu arah.
4	Djebaili Karima & Melkemi Lamine	Two Dimensional Elgamal Public Key Cryptosystem	2019	Varian baru enkripsi Elgamal dengan keamanan yang sangat sederhana
5	Edwin R. Arboleda	Secure and Fast Chaotic El Gamal Cryptosystem	2019	Pengabungan dua skema enkripsi yaitu kombinasi dari kriptografi Secure and Fast Chaos dan kriptografi El Gamal.

6	Andysah Putera Utama Siahaan	Comparative Analysis of RSA and Elgamal Cryptographic Public-key Algorithms	2019	Analisa perbandingan penggunaan kunci antara algoritma RSA dan Elgamal.
7	E. Jincharadze	Hybrid Encryption Model of Symmetric and Asymmetric Cryptography With AES and Elgamal Encryption Algorithms	2018	Model hybrid yang memiliki kinerja yang lebih baik mengggunakan AES dan Elgamal
8	Yuling Luo	An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems	2019	Objek yang diamankan berupa gambar (*image*)
9	Motilal Singh Khoirom	Audio Encryption Using Ameliorated Elgamal Public Key Encryption Over Finite Field	2021	Objek yang diamankan berupa file audio.
10	Raghi K.R, dan Arjun Paramarthalingam	Security using Mining Algorithm for Encrypted Data in Cloud Environment	2022	Objek yang diamankan berupa database.

II.2. Keamanan Komputer

Bidang keamanan komputer secara terus menerus mengalami perkembangan luar biasa sebab teknologi informasi memiliki pengaruh yang semakin tinggi terhadap bagaimana kita bekerja, berkomunikasi, berbelanja dan menikmati hiburan. Seiring dengan perkembangan itu maka semakin besar pula ancaman-ancaman terhadap keamanan komputer kita, baik ancaman berupa fisik maupun non fisik seperti *security hole* pada sistem operasi, serangan pada jaringan, virus, dan lain-lain. Dalam membangun sebuah sistem jaringan berbasis internet, masalah keamanan menjadi suatu hal yang mutlak diperlukan. Sistem yang dibangun tanpa adanya sistem keamanan yang baik sama halnya dengan

mengajak pencuri untuk masuk ke rumah kita dan membiarkan dia mengambil segala sesuatu yang kita miliki. Seringkali ketika membangun sebuah sistem, kita menemukan berbagai kerawanan dalam sistem kita. Namun hal itu kita anggap sebagai hal kecil karena kita tidak menganggapnya sebagai lubang keamanan (*hole*). Kita tidak sadar bahwa kerawanan-kerawanan kecil seperti inilah yang dimanfaatkan oleh orang-orang yang tidak bertanggungjawab untuk menjalankan aksi kejahatannya (Hasibuan, 2018).

Aspek-aspek keamanan komputer meliputi delapan aspek, antara lain (Hasibuan, 2018):

1. *Authentication*, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.
2. *Integrity*, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.
3. *Non-repudiation,* merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. *Authority*, informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
5. *Confidentiality*, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
6. *Privacy*, lebih ke arah data-data yang bersifat pribadi.

7. *Availability*, aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
8. *Access Control*, aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password* ataupun dengan mekanisme lain.

II.2.1. Keamanan Sistem Informasi

Apabila anda telah memiliki sebuah sistem informasi, pada bahasan ini akan membantu anda untuk mengevaluasi keamanan sistem informasi yang anda miliki. Meski sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah keamanan harus selalu di monitor. Hal ini disebabkan oleh beberapa hal, antara lain (Rahardjo, 1999):

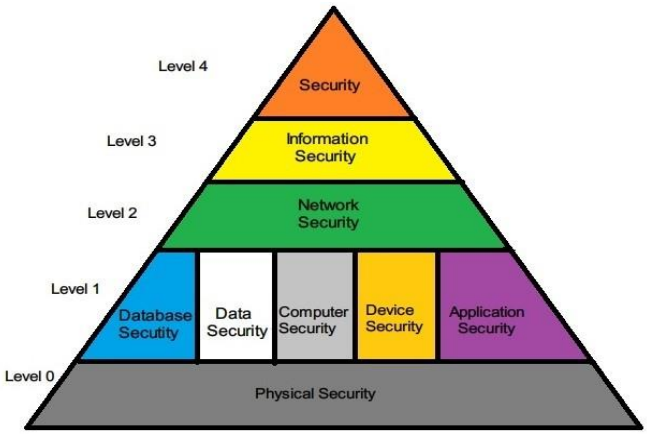
1. Ditemukannya lubang keamanan (*security hole*) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang – kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.
2. Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (*permission* atau kepemilikan) dari berkas yang menyimpan *password* (/etc/passwd di system UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.

3. Penambahan perangkat baru (*hardware* dan/atau *software*) yang menyebabkan menurunnya tingkat security atau berubahnya metoda untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya *server* atau *software* masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme "*access control*". Implementasi dari mekanisme ini antara lain dengan menggunakan "*password*". Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik adalah *firewall*. Filter dapat digunakan untuk memfilter e-mail, informasi, akses, atau bahkan dalam *level packet* (Rahardjo, 1999).

Salah satau mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang anda kirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di Internet yang masih menggunakan "*plain text*" untuk *authentication*, seperti penggunaan pasangan *userid* dan *password*. Informasi ini dapat dilihat dengan mudah oleh program penyadap (*sniffer*) (Rahardjo, 1999).

Berikut ini metodologi keamanan sistem informasi yang dijabarkan dalam bentuk piramida level keamanan.



Gambar 2.1. Piramida Level Keamanan

Terdapat 5 level Keamanan Sistem Informasi, yaitu :

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.
2. 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.
3. 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.

4. 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.
5. 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 dan lain – lain.

II.2.2. Keamanan Sistem World Wide Web

Keamanan *server* WWW biasanya merupakan masalah dari seorang *administrator*. Dengan memasang *server* WWW di sistem anda, maka anda membuka akses (meskipun secara terbatas) kepada orang luar. Apabila server anda terhubung ke Internet dan memang *server* WWW anda disiapkan untuk publik, maka anda harus lebih berhati-hati (Rahardjo, 1999).

Server WWW menyediakan fasilitas agar client dari tempat lain dapat mengambil informasi dalam bentuk berkas (*file*), atau mengeksekusi perintah (menjalankan program) di server. Fasilitas pengambilan berkas dilakukan dengan perintah “GET”, sementara mekanisme untuk mengeksekusi perintah di server

dikenal dengan istilah “CGI-bin” (*Common Gateway Interface*). Kedua servis di atas memiliki potensi lubang keamanan yang berbeda (Putra & Ariffin, 2019).

Adanya lubang keamanan di sistem WWW dapat dieksploitasi dalam bentuk yang beragam, antara lain : (Rahardjo, 1999)

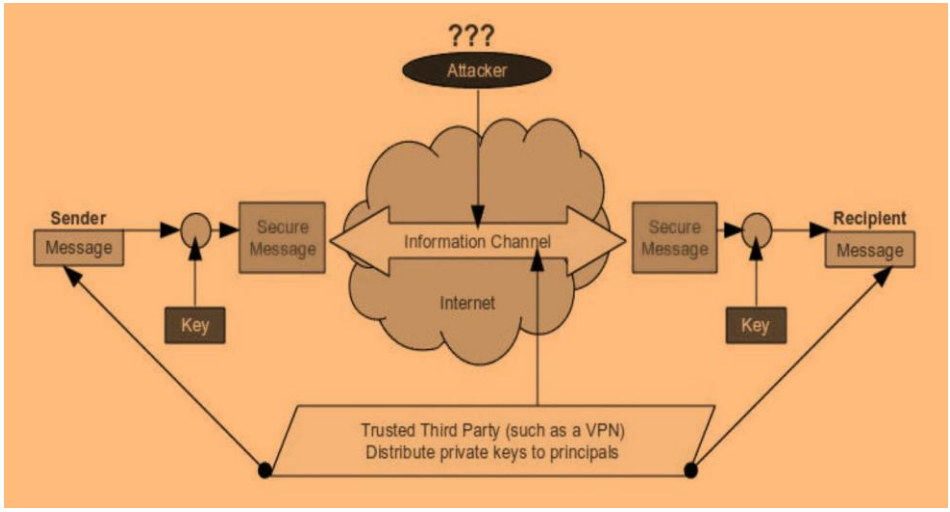
1. Informasi yang ditampilkan di server diubah sehingga dapat mempermalukan perusahaan atau organisasi anda;
2. Informasi yang semestinya dikonsumsi untuk kalangan terbatas (misalnya laporan keuangan, strategi perusahaan anda, atau database client anda) ternyata berhasil disadap oleh saingan anda;
3. Informasi dapat disadap (seperti misalnya pengiriman nomor kartu kredit untuk membeli melalui www);
4. Server anda diserang sehingga tidak bisa memberikan layanan ketika dibutuhkan (*denial of service attack*);
5. Untuk *server web* yang berada di belakang firewall, lubang keamanan di *server web* yang dieksploitasi dapat melemahkan atau bahkan menghilangkan fungsi dari *firewall*.

II.2.3. Keamanan Jaringan (*Network Security*)

Kriptografi adalah strategi untuk menyimpan dan mentransmisikan informasi dalam kerangka tertentu sehingga mereka yang diharapkan dapat membaca dan memprosesnya. Istilah ini secara teratur dihubungkan dengan pesan *plaintext scrambling* (konten tradisional, dalam beberapa kasus disinggung

sebagai *cleartext*) ke dalam *ciphertext* (prosedur yang disebut enkripsi), lalu kembali sekali lagi (dikenal sebagai *decoding*) (Setyapuji Winarno, 2019).

Model keamanan jaringan ditunjukkan dengan sebuah pesan akan dipertukarkan dimulai dengan satu titik ke titik lain melalui jaringan administrasi Internet seperti di tunjukkan pada gambar 2.2.



Gambar 2.2. Network Security Model

Sistem analisis keamanan jaringan (*network security*) mengimplementasikan kerangka kerja analitik volume data kecepatan tinggi dan tinggi yang menelan dan menganalisis beragam data jaringan, seperti *data Net Flow*, data DNS, dan data informasi keamanan dan manajemen. Sistem mendeteksi, kategori, dan melaporkan aktivitas yang tidak normal. Sistem ini menerapkan teknik pemrosesan bahasa alami (NLP) yang memeriksa konten analisis jaringan dan deret waktu untuk menetapkan dan mempertahankan model kondisi jaringan jaringan (misalnya, "normal" atau nominal). Sistem melakukan

analisisnya terhadap perspektif multi-dimensi dari aktivitas jaringan. (Joyce dan Ci, 2019)

II.3. Kriptografi

Keamanan menjadi masalah utama yang dihadapi setiap orang yang menggunakan internet dalam pekerjaan sehari-hari, keamanan bisa dicapai melalui lima kategori utama, yaitu :(AbdElminaam, 2018)

1. Otentikasi, yaitu pengguna yang tidak sah tidak dapat mengakses situs Anda atau jaringan Anda.
2. Otorisasi, hanya pengguna otentikasi yang diizinkan mengakses informasi.
3. Integritas, periksa apakah tanggal pengiriman tidak memiliki modifikasi dalam cara penerima, dan data ini masih berlaku.
4. Audit, evaluasi sistematis keamanan informasi.
5. Ketersediaan, paling baik dipastikan dengan menjaga informasi atau data dengan ketat.

Perkembangan ilmu pengetahuan dan teknologi khususnya teknologi informasi dan komunikasi membawa perubahan besar pada gaya hidup manusia. Akan tetapi kemudahan penggunaan teknologi tersebut kurang diiringi dengan kesadaran pengamanan yang memadai. Hal ini mengakibatkan ancaman terhadap keamanan data dan informasi sangat besar. Salah satu alat yang dapat digunakan untuk mengamankan data dan informasi adalah kriptografi. Layanan keutuhan data dapat mendeteksi manipulasi yang dilakukan terhadap suatu data oleh pihak

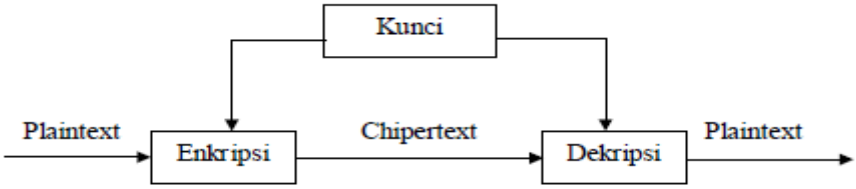
yang tidak berhak. Manipulasi data mencakup penyisipan (*insertion*), penghapusan (*deletion*) dan substitusi (*substitution*) (Yusfrizal, 2018).

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Karman dan Nurhasan, 2019)

Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia. Sebuah pesan asli yang disebut sebagai *plaintext* disandikan menjadi pesan yang tersandi yang disebut sebagai *ciphertext* melalui proses enkripsi dan *ciphertext* dipulihkan menjadi *plaintext* kembali melalui proses dekripsi. Kriptografi memiliki beragam algoritma yang telah banyak digunakan sebagai keamanan untuk informasi. Algoritma kriptografi dikelompokkan ke dalam dua jenis yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Dalam pengoperasiannya, algoritma kriptografi klasik bekerja menggunakan mode karakter sedangkan algoritma kriptografi modern bekerja menggunakan mode *bit* (Yusfrizal, 2019).

Kriptografi memiliki dua konsep utama, yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah proses penyandian plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi

plainteks semula. Enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk *transformasi* (Yusfrizal, 2019).



Gambar 2.3. Skema Enkripsi dan Dekripsi Kriptografi *Type Symmentric Key*

Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah *informasi* rahasia, disebut sebagai kunci. Untuk beberapa *mekanisme* enkripsi, kunci yang sama digunakan baik untuk enkrispi dan dekripsi; untuk *mekanisme* yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua *tipe* dasar dari *teknologi* kriptografi adalah *symmentric key* (*secret/private key*) *cryptography* dan *asymmetric* (*public key*). Pada *symmentric key cryptography*, baik pengirim maupun penerima memiliki kunci rahasia yang umum. pada *asymmentric key cryptography*, penerima masing-masing berbagi kunci *public* dan *private*. Kriptografi saat ini lebih dari enkripsi dan dekripsi saja (Yusfrizal, 2019).

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi adalah (Yusfrizal, 2019):

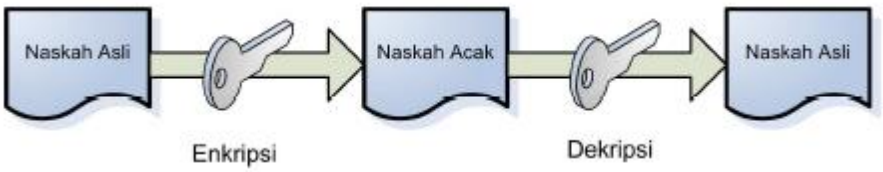
1. Kerahasiaan, layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.
2. Integritas Data, berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk dapat menjaga integritas 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, berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus di Otentikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.
4. Non-repudiasi, merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat (Yusfrizal, 2019).

II.3.1. Algoritma Kriptografi Klasik

Algoritma kriptografi klasik memiliki ciri di antaranya berbasis karakter dan menggunakan kunci simetri. Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi seperti dapat dilihat pada Gambar 2.4. (Yusfrizal, 2019)



Gambar 2.4. Proses Enkripsi dan Dekripsi

Salah satu algoritma klasik adalah *Caesar Cipher*. Dalam kriptografi klasik, secara umum dapat dikelompokkan dalam dua model yaitu menggunakan tekik substitusi dan transposisi. Teknik substitusi dilakukan dengan mengganti

salah satu karakter yang ada dalam sebuah teks menggunakan karakter yang lain. Teknik yang termasuk dalam kategori substitusi adalah kriptografi *Caesar* (Hamdah et al., 2020).

II.3.2. Algoritma Kriptografi Modern

Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol *biner* yang dibentuk dari kode ASCII (*American Standard Code for Information Interchange*) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya. Algoritma ini memiliki tingkat kesulitan yang kompleks yang menyebabkan kriptanalis sangat sulit memecahkan *ciphertext* tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: simetri, asimetri, dan hibrida. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Contoh kriptografi modern yaitu MD5, RC4, AES dan lain-lain (Saragih, 2021).

Berikut akan dijelaskan jenis – jenis kunci dalam kriptografi modern adalah sebagai berikut (Saragih, 2021):

1. Algoritma Simetris, adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk

enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya relatif cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara *real time* seperti GSM. Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma seperti Data Encryption Standard (DES), Advance Encryption Standard (AES), International Data Encryption Algoritma (IDEA), A5, dan lain – lain.

2. Algoritma Asimetris, adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi lagi deskripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia, untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (merupakan singkatan dari nama penemunya, yakni Rivest, Shamir dan Adleman).
3. Algoritma Hibrida, adalah algoritma yang memanfaatkan dua tingkatan kunci, yaitu kunci rahasia (simetri) – yang disebut juga *session key* (kunci sesi) untuk enkripsi data dan pasangan kunci rahasia – kunci publik untuk pemberian tanda tangan digital serta melindungi kunci simetri.

II.4. Algoritma Elgamal

Algoritma Elgamal ditemukan pada tahun 1985 oleh ilmuwan Mesir yaitu Taher Elgamal. Algoritma Elgamal merupakan algoritma berdasarkan konsep kunci publik. Algoritma ini pada umumnya digunakan untuk *digital signature*,

namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi. Keamanan algoritma Elgamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah algoritma ini menjadi sulit untuk dipecahkan. Algoritma ini memiliki kelebihan yaitu pembangkitan kunci yang menggunakan logaritma diskrit dan metode enkripsi dekripsi yang menggunakan proses komputasi yang besar sehingga hasil enkripsinya berukuran dua kali dari ukuran semula. Kekurangan algoritma ini adalah membutuhkan *resource* yang besar karena cipherteks yang dihasilkan dua kali panjang plainteks serta membutuhkan procesor yang mampu untuk melakukan komputasi yang besar untuk perhitungan logaritma perpangkatan besar. (Sari et al., 2018)

Proses pembentukan kunci algoritma Elgamal adalah sebagai berikut (Nguyen Duc dan Bui, 2017) :

1. Pilih bilangan prima *p* cukup besar sehingga masalah logaritma *Zp* sulit dipecahkan.
2. Pilih $g \varepsilon Z^*p$ sebagai elemen primitif.
3. Pilih kunci rahasia x sebagai angka acak sedemikian rupa sehingga :

   $1 < x < p$ ..... (II.1)

Algoritma Elgamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan.

II.4.1. Proses Pembentukan Kunci

Pembentukan kunci terdiri atas pembentukan kunci publik dan kunci rahasia. Pada proses ini dibutuhkan sebuah bilangan prima *p* yang digunakan untuk membentuk grup *Zp**, elemen primitif α dan sembarang $a \in \{0,1,..., p-2\}$. Kunci publik algoritma Elgamal terdiri atas pasangan 3 bilangan (p, α , β) dimana :

$$\beta = \alpha^a \bmod p \quad \text{..... (II.2)}$$

Sedangkan kunci rahasianya adalah bilangan *a* tersebut. Proses pembentukan kunci untuk algoritma Elgamal terdiri atas :

1. Penentuan Bilangan Prima Aman Besar

   Tujuan penentuan bilangan prima aman ini adalah untuk mempermudah dalam penentuan elemen primitif. Digunakan bilangan prima *p* sehingga :

   $$p = 2.q + 1 \quad \text{..... (II.3)}$$

   dengan *q* adalah bilangan prima sehingga nilai minimal *p* adalah 5 dan *q* adalah 2. Bilangan prima *p* tersebut disebut sebagai bilangan prima aman. Langkah penentuan bilangan prima tersebut dinyatakan sebagai berikut:

   a. Tentukan bilangan prima $p \geq 5$
   b. Hitung *q* dengan “persamaan (2)”
   c. Jika *q* merupakan bilangan prima, maka *p* merupakan bilangan prima aman.
   d. Jika *q* bukan merupakan bilangan prima, maka *p* bukan merupakan bilangan prima aman.

Untuk menguji keprimaan suatu bilangan, digunakan suatu metode yang disebut Teorema Fermat. Jika *x* adalah bilangan prima dan *y* adalah bilangan bulat yang tidak habis dibagi dengan *x*, yaitu PBB(*y*,*x*) = 1, maka :

$y^{x-1} \equiv 1 \ (\text{mod } p)$ ..... (II.4)

Contoh pengujian keprimaan suatu bilangan. Diuji apakah 17 dan 21 bilangan prima atau bukan. Kemudian diambil nilai *a* = 2 karena PBB (17,2) = 1 dan PBB(21,2) = 1. Untuk 17, $2^{17-1} = 65536 \equiv 1$ (mod 17) Karena 17 habis membagi 65536 – 1 = 65535 (65535 ÷ 17= 3855). Untuk 21, $2^{21-1} = 1048576 \equiv\backslash\ 1$ (mod 21). Karena 21 tidak habis membagi 1048576 – 1 = 1048576. Akan tetapi, teorema ini memiliki kekurangan karena terdapat bilangan komposit *n* sedemikian sehingga $2^{n-1} \equiv 1$(mod *n*). Bilangan itu disebut bilangan prima semu (*pseudoprimes*). Mislanya komposit 341 (yaitu 341 = 11.31) adalah bilangan prima semu menurut teoreme Fermat,$2^{340} \equiv 1$ (mod 340). Namun, bilangan prima semu ini relatif jarang terdapat.

2. Penentuan Elemen Primitif

Teorema : "Suatu elemen yang membangun Z*p* * disebut *elemen primitif (primitive root) mod p*. "Bila $\alpha^2 \bmod p \neq 1$ dan $\alpha^q \bmod p \neq 1$. Jika keduanya dipenuhi, maka α adalah elemen primitif dari Z*p* *". Langkah penentuan elemen primitif tersebut dapat dinyatakan sebagai berikut :

a. Tentukan bilangan prima $p \geq 5$ dan $\alpha \in Zp$ *
b. Hitung *q* dengan "p = 2.q + 1"
c. Hitung $\alpha^2 \bmod p$ dan $\alpha^q \bmod p$.

d. Jika $\alpha^{2} \bmod p = 1$ atau $\alpha^{q} \bmod p = 1$, maka α bukan merupakan elemen primitif.

e. Jika $\alpha^{2} \bmod p \neq 1$ dan $\alpha^{q} \bmod p \neq 1$, maka α bukan merupakan elemen primitif.

3. Pembentukan Kunci Berdasarkan Bilangan Prima Aman dan Elemen Primitif

Setelah bilangan prima aman dan elemen primitive diperoleh, kunci publik dan kunci rahasia untuk algoritma Elgamal dapat dibentuk. Algoritma Elgamal dalam prosesnya menggunakan bilangan bulat untuk perhitungan. Oleh karena itu, pesan yang terkandung dalam plainteks harus dalam bentuk bilangan bulat. Untuk memenuhi persyaratan tersebut, digunakan kode ASCII *(American Standard for Information Interchange)* yang merupakan *representasi numeric* dari karakter – karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255.

Selanjutnya, dengan kondisi – kondisi tersebut, pembentukan kunci dapat dibentuk dengan mengacu pada langkah berikut :

a. Tentukan bilangan prima $p \geq 5$ dan $\alpha \in Zp^{*}$

b. Pilih $a \in \{0,1,..., p-2\}$ sembarang.

c. Hitung nilai β dengan rumus :

$$\beta = \alpha^{a} \bmod p \quad \text{..... (II.5)}$$

Diperoleh kunci publik (p, α ,β) yang dapat dipublikasikan serta nilai kunci rahasia a yang dirahasiakan nilainya. Pihak yang membuat kunci publik dan kunci rahasia merupakan pihak penerima pesan. Sedangkan pihak pengirim

hanya mengetahui kunci publik dari penerima untuk mengenkripsi pesan yang akan dikirim.

II.4.2. Proses Enkripsi

Proses enkripsi menggunakan kunci publik (p, α, β) dan sebuah bilangan integer acak k ($k \in \{0,1,..., p-1\}$) yang dijaga kerahasiaannya oleh penerima yang mengenkripsi pesan. Untuk setiap karakter dalam pesan dienkripsi dengan menggunakan bilangan k yang berbeda-beda. Satu karakter yang direpresentasikan dengan menggunakan bilangan bulat ASCII akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (r, t).

Langkah proses enkripsi :

1. Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter tersebut kedalam kode ASCII sehingga diperoleh bilangan bulat M.
2. Hitung nilai r dan t dengan persamaan berikut:

   $r = \alpha^{k} \pmod{p}$ .....(2.6)

   $t = \beta^{k} M \pmod{p}$ .....(2.7)
3. Diperoleh cipherteks untuk karakter M tersebut dalam blok (r, t)
4. Lakukan proses di atas untuk seluruh karakter dalam pesan termasuk karakter spasi.

II.4.3. Proses Dekripsi

Dekripsi dari cipherteks ke plainteks menggunakankunci rahasia a yang disimpan kerahasiaanya oleh penerima pesan. Teorema : Diberikan (p, α, β)

sebagai kunci *public* dan *a* sebagai kunci rahasia pada algoritma Elgamal. Jika diberikan cipherteks (*r, t*) maka :

$$M = t\,(r^a)^{-1} \bmod p \quad \text{.....(2.8)}$$

dengan *M* adalah plainteks.

Di mana nilai :

$$(r^a)^{-1} = r^{-a} = r^{p-1-a} \bmod pBI \quad \text{.....(2.9)}$$

Langkah proses dekripsi:

1. Ambil sebuah blok cipherteks dari pesan yang telah dienkripsikan pengirim.
2. Dengan menggunakan *a* yang dirahasiakan olehpenerima, hitung nilai plainteks dengan menggunakan "$M = t\,(r^a)^{-1} \bmod p$" dan "$(r^a)^{-1} = r^{-a} = r^{p-1-a} \bmod p$)".

II.4.4. Penerapan Algoritma Elgamal

Sebagai ilustrasi dari algoritma Elgamal tersebut, algoritma tersebut diaplikasikan pada sebuah kasus. Misal kasus tersebut: "Alice ingin saling berkomunikasi dengan Bob. Suatuhari ia ingin mengirimkan sebuah pesan rahasia untuk Bob agar tidak diketahui orang lain. Alice menggunakan algoritma Elgamal untuk menyamarkan pesan yang akan disampaikan. Pesan tersebut,"SELAMAT PAGI".

Ditunjukkan proses penyamaran pesan tersebut melalui langkah-langkah yang telah disebutkan.

1. Pembentukan kunci oleh penerima pesan

Pembentukan kunci publik dan kunci rahasia dilakukan oleh penerima pesan yaitu Alice. Langkah-langkah yang dilakukan Alice dalam pembentukan kunci:

a. Menentukan bilangan prima aman *p*, disarankan ambil nilai *p* yang besar. Diambil nilai $p = 107$.
b. Alice mengecek apakah *p* termasuk bilangan prima aman atau tidak dengan mencari nilai *q*. Diperoleh nilai $q = 53$ yang juga merupakan bilangan prima. Oleh karena itu, Alice menyimpulkan *p* merupakan bilangan prima aman.
c. Selanjutnya Alice mencari elemen primitif α dariZ_p^*.
d. Alice membuat tabel perhitungan untuk beberapa nilai α untuk mengecek apakah nilai tersebut termasuk elemen primitif atau tidak.

Tabel 2.2. Perhitungan α^2 *mod p* dan α^q *mod p*

α	2	3	4	5	6
α^2 mod p	4	9	16	25	36
α^q mod p	106	1	1	106	106

e. Dari beberapa nilai tersebut Alice mendapatkan beberapa nilai α dari Z_p^* yaitu 2, 5 dan 6. Alice memilih nilai α yang dipakai sebagai elemen primitif adalah $\alpha = 2$. Kemudian Alice menentukan kunci rahasia *a* (dimana $a \in \{0,1,..., p-2\}$) dengan nilai 63 sehingga sekarang Alice mempunyai nilai $(p, \alpha, a) = (107,2, 63)$.
f. Dengan nilai *a* yang sudah diketahui, Alice mencari nilai β.

   $\beta = \alpha^a \ mod \ p$

   $\beta = 2^{63} \ mod \ 107$

$\beta = 46$.

g. Alice mendapatkan kunci publik $(p, \alpha, \beta) = (107, 2, 46)$ dan kunci rahasia $a = 63$. Kunci publik tersebut diberitahukan ke Bob untuk mengenkripsi pesan yang akan dikirim Bob ke Alice dan kunci rahasia dijaga keamanannya oleh Alice.

2. Enkripsi pesan oleh pengirim

Bob menerima kunci publik dari Alice $(p, \alpha, \beta) = (107, 2, 46)$. Dengan kunci publik tersebut, Bob mengenkripsi pesan "SELAMAT PAGI" untuk dikirimkan ke Alice. Langkah-langkah yang dilakukan Bob dalam mengenkripsi pesan tersebut:

a. Pertama Bob mengonversi pesan tersebut dalam kode ASCII.

Tabel 2.3. Konversi Karakter ke Kode ASCII

i	karakter	Plainteks M_i	ASCII
1	S	M_1	83
2	E	M_2	69
3	L	M_3	76
4	A	M_4	65
5	M	M_5	77
6	A	M_6	65
7	T	M_7	84
8	<spasi>	M_8	32
9	P	M_9	80
10	A	M_{10}	65
11	G	M_{11}	71
12	I	M_{12}	73

b. Kemudian Bob menentukan bilangan acak k ($k \in \{0,1,..., 106\}$) yang dijaga kerahasiaannya untuk setiap plainteks M dan mengenkripsi plainteks tersebut dengan menghitung nilai r dan t.

Tabel 2.4. Enkripsi Plainteks ke Cipherteks

i	M_i	k_i	$r = 2^k \pmod{107}$	$t = 46^k M_i \pmod{107}$
1	83	57	91	21
2	69	43	7	78
3	76	65	77	82
4	65	88	89	66
5	77	34	9	98
6	65	46	56	93
7	84	47	5	4
8	32	76	85	22
9	80	87	98	83
10	65	69	55	23
11	71	41	82	11
12	73	35	18	23

c. Berdasarkan tabel tersebut, Bob memperoleh cipherteks (*ri, ti*), *i* = 1, 2, …, 12 sebagai berikut:

(91, 21), (7, 78) (77, 82) (89, 66) (9, 98) (56, 93)(5, 4)(85, 22) (98, 83) (55, 23) (82, 11) (18, 23)

d. Selanjutnya cipherteks tersebut dikirimkan ke Alice.

Tampak bahwa dengan menggunakan bilangan integer acak yang berbeda akan menghasilkan cipherteks yang berbeda pula. Namun, ketika cipherteks tersebut didekripsi, akan diperoleh plainteks yang sama.

3. Dekripsi pesan oleh penerima

Alice memperoleh pesan yang telah disamarkan dari Bob. Karena Alice yang memegang kunci rahasia (*a* = 63) dari enkripsi tersebut, Alice dapat mendekrip pesan tersebut agar dapat dibaca. Alice melakukan perhitungan untuk tiap blok cipherteks.

Tabel 2.5. Dekripsi Cipherteks ke Plainteks

i	r	t	$r^{43} \bmod 107$	$M_i = t\, r^{43} \bmod 107$	Karakter M_i
1	91	21	60	83	S
2	7	78	5	69	E
3	77	82	74	76	L
4	89	66	48	65	A
5	9	98	39	77	M
6	56	93	3	65	A
7	5	4	21	84	T
8	85	22	89	32	<spasi>
9	98	83	68	80	P
10	55	23	54	65	A
11	82	11	94	71	G
12	18	23	59	73	I

Berdasarkan tabel tersebut, Alice memperoleh plainteks dari pendekripsian cipherteks yang diberikan Bob. Pesan yang hendak disampaikan Bob: "SELAMAT PAGI".

II.5. Keamanan Database

Database merupakan kumpulan informasi informasi yang disimpan didalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu proram untuk memperoleh informasi dari basis data tersebut. Pengertian umum dari Database adalah sistem penyimpanan data dimana data yang sudah banyak di input disiman dalam satu sistem penyimpanan. Sistem database sudah banyak digunakan dibanyak bidang, tidak hanya bidang teknologi, bahkan saat ini database sudah digunakan diperusahaan dari yang keil hingga besar, universitas, perkantoran, supermarket bahkan rumah-rumah (Simanjuntak, 2019).

Basis data adalah akumulasi data yang disusun dengan cara bahwa program komputer dapat dengan cepat memilih *bit* yang diinginkan informasi. Pengguna dapat berpikir tentang database sebagai elektronik mendokumentasikan

kerangka kerja. Ini adalah kumpulan data yang dapat diakses oleh klien atau pengguna resmi dalam berbagai metode. Datanya adalah proses dan disimpan sebagai informasi dalam manajemen basis data sistem (DBMS) (Yunus et. al, 2017).

Ada beberapa jenis teknik untuk keamanan sistem manajemen basis data, teknik yang diusulkan adalah *watermarking* untuk kepemilikan. Pemilik dapat melindungi data dengan memasukkan gambar *watermarking* ke dalam basis data selama serangan berbahaya untuk mencuri data. Selain itu, enkripsi basis data adalah cara untuk mengubah informasi di dalam sistem manajemen basis data, dalam konfigurasi konten sederhana menjadi pesan angka yang tidak penting dengan metode untuk perhitungan yang sesuai. Data yang dienkripsi rentan terhadap berbagai serangan yang tidak memerlukan akses ke kunci dekripsi. Dekripsi basis data berubah dari konten gambar tanpa tujuan menjadi data pertama yang menggunakan kunci yang dihasilkan oleh perhitungan enkripsi. Tujuan enkripsi dan dekripsi adalah untuk melindungi kerahasiaan data dan untuk menjaga integritas data pelanggan melalui layanan keamanan basis data. Peran enkripsi data adalah untuk memastikan kerahasiaan data (Yunus et al., 2017).

SQL Server 2008 adalah sebuah terobosan baru dari Microsoft dalam bidang database. SQL Server adalah DBMS (*Database Management System*) yang dibuat oleh Microsoft untuk ikut berkecimpung dalam persaingan dunia pengolahan data menyusul pendahulunya seperti IBM dan Oracle. SQl Server 2008 dibuat pada saat kemajuan dalam bidang hardware sedemikian pesat. Oleh karena itu sudah dapat dipastikan bahwa SQL Server 2008 membawa beberapa

terobosan dalam bidang pengolahan dan penyimpanan data. Microsoft merilis SQL Server 2008 dalam beberapa versi yang disesuaikan dengan segment-segment pasar yang dituju (Kurniawan, 2015)