BAB II

TINJAUAN PUSTAKA

2.1 *E-Voting*

Voting merupakan salah satu cara pengambilan keputusan dengan penentuan dari suara terbanyak dari seluruh anggota di suatu organisasi. Dalam *e-voting* (*voting* secara elektronik) proses pemungutan suaranya dilakukan dengan cara pemilih memberikan suara melalui Internet atau Intranet. *E-Voting* merupakan suatu aplikasi atau sistem yang digunakan untuk melakukan *voting* secara elektronik. Pelaksanaan *voting* menggunakan *e-voting* dilakukan dengan melakukan pembuatan akun untuk para pemilih, kegiatan pemilihan, perhitungan perolehan suara dan menampilkan hasil perolehan suara secara elektronik. Hasil perolehan suara pada *e-voting* biasanya disajikan secara digital berbentuk diagram.

Electronic election system harus mengutamakan kerahasiaan dan keamanan. Jika kerahasiaan dan keamanan dapat terjamin, maka *e-voting* sudah tepat untuk digunakan. (García-Zamora et al., 2005) Terdapat beberapa aspek manfaat dari penerapan *e-voting* yaitu sebagai berikut. (Zafar & Pilkjaer, 2007)

a. Biaya: sumber daya yang lebih menghemat dibandingkan dengan *voting* manual yang kurang efisien.
b. Waktu: waktu pelaksanaan yang lebih cepat dibandingkan *voting* manual.
c. Hasil: hasil perolehan suara yang lebih tepat, akurat dan mengurangi risiko terjadinya *human error* denagn sistem yang baik.

2.2 Kriptografi

Kriptografi merupakan ilmu untuk mengamankan pesan ketika pesan tersebut dikirim dari suatu pengirim ke penerima. (Dony Ariyus, 2008)

Kriptografi ialah suatu ilmu pengetahuan yang menggunakan persamaan matematika untuk melakukan penyandian pesan (Purbo, W & Wahyudi, 2000). Kriptografi memiliki tujuan untuk menjamin keamanan isi data dengan menjaga kerahasiaan suatu informasi dari pihak yang tidak memiliki hak untuk melihat isi

pesan tersebut. Dengan menggunakan suatu algoritma dapat dilakukan enkripsi (*encrypt*) yaitu pesan diganti menjadi pesan sandi yang sudah sangat berbeda dengan pesan aslinya. Pihak yang memiliki wewenang untuk menerima pesan harus mengetahui algoritma dan juga kunci yang digunakan untuk menjadikan pesan sandi ke bentuk pesan aslinya, proses tersebut dikenal dengan istilah dekripsi (*decrypt*). Penggunaan algoritma dan pemilihan kunci yang digunakan sangat mempengaruhi tingkat keamanan pesan yang sudah tersandi, pihak yang tidak memiliki kewenangan untuk mengakses akan mengalami kesulitan dalam melakukan proses dekripsi secara paksa.

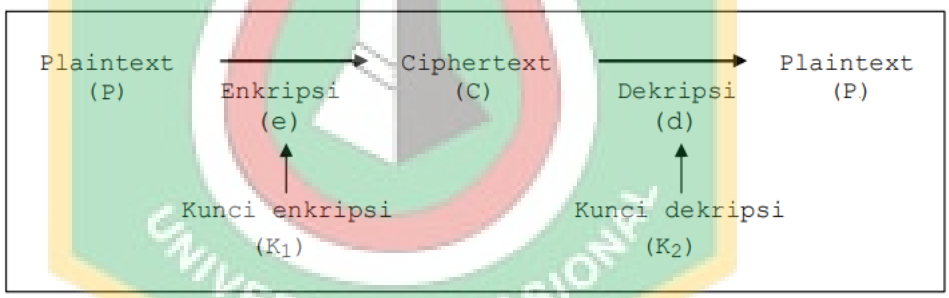
Kerumitan algoritma yang diimplementasikan ketika enkripsi dan dekripsi sangat erat hubungannya dengan persamaan matematika. Semakin rumit perhitungan yang digunakan maka pesan sandi yang muncul akan sangat aman.(Menezes et al., 1996)

Beberapa istilah yang berhubungan erat dengan kriptografi sebagai berikut.(Purbo, W & Wahyudi, 2000)

a. *Plaintext / cleartext* merupakan data asli yang isi datanya dapat dibaca dan dimengerti. Data tersebut yang akan menjadi data utama untuk proses enkripsi.
b. *Ciphertext* merupakan data yang dihasilkan dari proses enkripsi.
c. *Cipher* merupakan algoritma yang digunakan untuk mengubah *plaintext* menjadi *ciphertext*. Hasil perubahan dapat berbentuk *substitution cipher*, *transposition cipher*, atau gabungan dari keduanya.
d. *Substitution cipher* merupakan algoritma yang mengubah *plaintext* menjadi *ciphertext* dengan cara mengganti.
e. *Transposition cipher* merupakan algoritma yang mengubah *plaintext* menjadi *ciphertext* dengan cara menggeser.
f. *Block Cipher* merupakan algoritma mengubah *plaintext* menjadi *ciphertext* untuk setiap *block data*. Jumlah data atau besarnya *block* adalah tertentu. Kunci (*key*) adalah data atau nilai spesifik yang hanya diketahui oleh pengirim dan penerima yang memiliki wewenang. Kunci digunakan untuk melakukan proses enkripsi dan dekripsi.

g. Enkripsi (*encryption*) merupakan proses untuk menyandikan *plaintext*. Hasil dari proses enkripsi adalah data sandi (*ciphertext*).
h. Dekripsi (*decryption*) kebalikan dari proses enkripsi yaitu mengembalikan *ciphertext* menjadi *plaintext*.
i. Kriptosistem (*cryptosystem*) merupakan sistem kriptografi yang terdiri dari: algoritma kriptografi, *plaintext*, *ciphertext*, *key*, dan beberapa unsur lain yang mempengaruhi sistem kriptografi.
j. *Cryptanalysis/code breaking* yaitu suatu kegiatan untuk menggganti *ciphertext* menjadi pesan aslinya tanpa mengetahui kunci yang sesuai, tetapi dilakukan dengan coba-coba (*trial and error*).
k. *Cryptology* adalah ilmu matematika yang mendasari *crypthography* dan *cryptanalysis*.

Pada gambar 2.1 merupakan alur proses enkripsi dan dekripsi yang menyertakan kunci(*key*).(Lingkup et al., 2004)



Gambar 2. 1 Alur Proses Enkripsi dan Dekripsi Dengan Kunci

Gambar 2.1 menerangkan proses enkripsi yaitu *plaintext* menjadi *chipertext* yang diproses menggunakan kunci. Begitu juga dengan proses dekripsi yaitu berkebalikan dengan proses enkripsi. Proses untuk menjadikan *plaintext* ke *chipertext* yang juga memakai kunci.

Proses enkripsi dapat ditulis dengan :

$$eK1\ (P) = C \quad (2.1)$$

Proses dekripsi dapat ditulis dengan :

$$dK2\ (C) = P \quad (2.2)$$

Proses pengujian dapat dilakukan dengan :

$$dK2\big(eK1(P)\big) = P \qquad (2.3)$$

2.3 *Caesar Chiper*

Algortima *Caesar Chiper* ialah kriptografi yang paling sederhana dan paling dikenal. Algortima ini termasuk teknik substitusi yaitu setiap huruf yang ada dalam *plaintext* diubah dengan huruf lain yang terdapat selisih posisi tertentu dalam alfabet. Dalam *Caesar cipher*, setiap huruf yang ada di *plaintext* diganti dengan huruf ketiga setelahnya dari susunan alfabet yang sama. Dapat ditentukan bahwa kunci yang digunakan adalah pergeseran huruf alfabet sejauh 3 (tiga). Berikut susunan alfabet yang telah digeser sejauh 3 huruf, sebagai berikut:

Alfabet Biasa: 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

Alfabet Sandi: 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

Untuk melakukan penyandian pesan dapat dilakukan dengan mencocokan huruf yang akan dienkripsi pada alfabet biasa, setelah itu tulis huruf yang susunannya cocok pada alfabet sandi. Untuk mengubah pesan sandi menjadi pesan yang asli, dapat menggunakan cara sebaliknya. Contohnya adalah sebagai berikut.

Plaintext : JAKARTA KOTA KOLABORASI

Chipertext : MDNDU WDNRW DNROD ERUDVL

Dengan memberikan kode setiap huruf pada alfabet dengan integer : ‘A’= 0 , ‘B’= 1,…, ‘Z’= 25, maka secara perhitungan matematika pergeseran 3 huruf alfabetik ekivalen dengan melakukan operasi modulo pada *plainteks* P menjadi *cipherteks* C dengan persamaan sebagai berikut

$$C = E(P) = (P + 3)\ mod\ 26 \qquad (2.4)$$

Terdapat 26 huruf yang ada pada alfabet. Penerima pesan akan mengembalikan *cipherteks* dengan rumus kebalikannya, yang dapat dinyatakan dengan persamaan berikut

$$P = D(C) = (C - 3)\ mod\ 26 \quad (2.5)$$

Dapat dilihat bahwa fungsi D merupakan balikan (invers) dari fungsi E, yaitu :

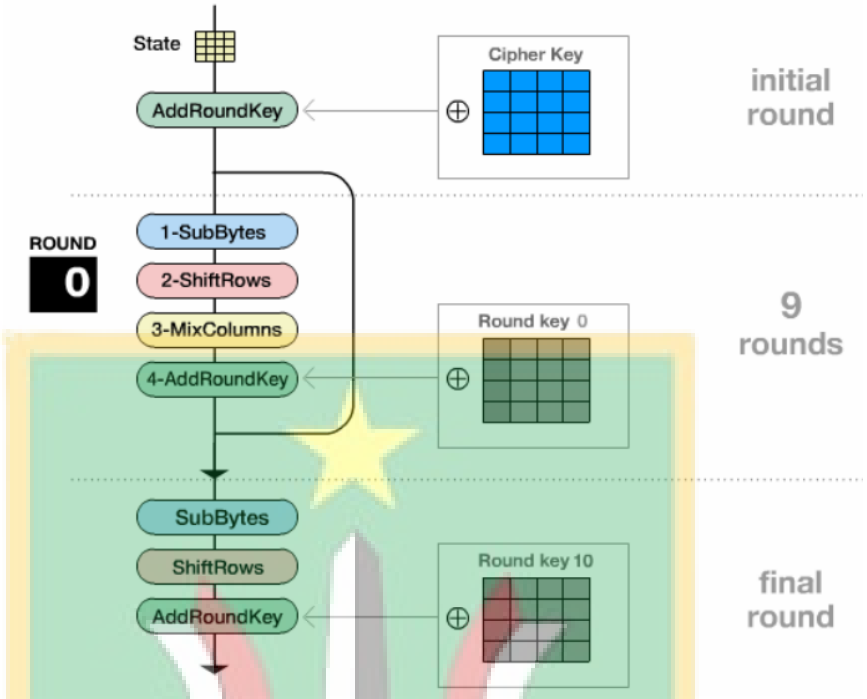
$$D(C) = E - 1(P) \quad (2.6)$$

2.4 *AES* (*Advanced Encryption Standard*)

Advanced Encryption Standard (AES) merupakan salah satu algoritma *cryptographic* unttuk dipergunakan dalam pengamanan data. Algoritma *AES* termasuk blok *chipertext* simetrik yang dapat melakukan proses enkripsi dan dekripsi data. Enkripsi adalah sebuah proses merubah data awal (*plaintext)* menjadi data yang disandikan (*chipertext*), kebalikannya proses dekripsi merupalan proses merubah *ciphertext* menjadi bentuk data awal yang disebut sebagai *plaintext*. Pada algoritma AES digunakan kunci kriptografi 128, 192, dan 256 bits untuk proses enkrip dan dekrip data pada blok 128 bits.(Ibrahim, 2017)

2.4.1 Proses Enkripsi

Proses enkripsi pada algoritma AES terdiri dari 4 jenis, antara lain *SubBytes, ShiftRows, Mixcolumns,* dan *AddRoundKey*. Proses enkripsi pertama yaitu memasukan yang telah disalinkan ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Kemudian, *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang sebanyak Nr. Proses tersebut dikenal dengan *round function* pada algoritma AES. Ketika round terakhir, *state* tidak mengalami *MixColumns*. Gambaran proses enkripsi pada algoritma AES dapat diperhatikan pada Gambar 2.2.



Gambar 2. 2 Alur Proses Enkripsi Algortima AES

Gambar 2.2 menjelaskan bagaimana alur proses enkripsi algoritma AES, tahapan pertama adalah *initial round* yaitu proses *AddRoundKey*. Tahapan selanjutnya adalah 9 *rounds* yaitu proses *SubBytes*, *ShiftRows*, *MixColums dam AddRoundKey*. Tahapan yang terakhir adalah *final round* yaitu proses *Round Key* 10. Pada *Round Key* 10 hanya tidak melewati proses *MixColumns*.

Tahapan Algoritma AES yang beroperasi pada blok 128-bit dengan kunci 128-bit (diluar proses pembangkitan *roundkey*) antara lain:

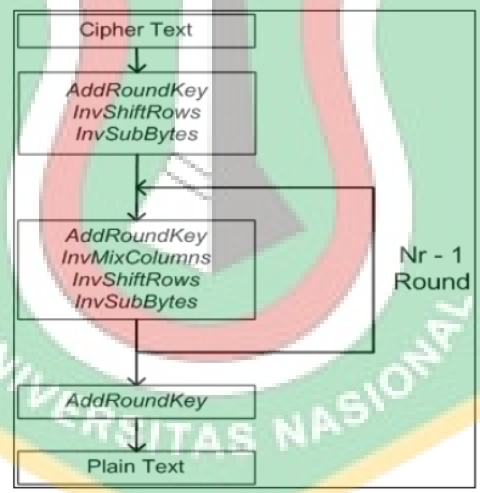
1. *AddRoundKey*, lakukan *XOR* antara awal (*plaintext*) dengan *cipher key*.
2. Melakukan p utaran sebanyak Nr-1 kali. Pada setiap putaran yang dilakukan adalah :
   a. *SubBytes* yaitu subsitusi *byte* menggunakan *table* subsitusi (*S-Box*).
   b. *ShiftRows* yaitu proses pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumns* yaitu proses mengacak data pada masing-masing kolom *array state*.

d. *AddRoundKey* yaitu melakukan *XOR* antara *state* sekarang *round key*.

3. *Final round*, proses untuk putaran terakhir :
   a. *SubBytes*
   b. *ShiftRows*
   c. *AddRoundKey*

2.4.2 Proses Dekripsi

Perubahan *cipher* dapat dikembalikan dan diimplementasikan dengan arah yang berkebalikan untuk mendapatkan invers *cipher*. Perubahan yang digunakan pada invers *cipher* yaitu *InvShiftRows, InvSubBytes, InvMixColumns,* dan *AddRoundKey*. Proses dekripsi pada algoritma AES dapat diperhatikan pada Gambar 2.3.(Ibrahim, 2017)



Gambar 2. 3 Alur Proses Dekripsi AES

Gambar 2.3 menjelaskan mengenai proses dekripsi pada algoritma AES. Prosesnya yaitu kebalikannya dari proses enkripsi. Pada tahap awal, *chipertext* akan melewati proses *AddRoundKey*, *InvShiftRows* dan *InvSubBytes* setelah itu dapat dilanjutkan ke tahapan berikutnya.

2.5 *MySQL*

MySQL adalah sistem *database* yang bisa diandalkan. Pertamanya, *SQL* digunakan sebagai bahasa yang menghubungkan antara program *database* dengan bahasa pemrograman yang digunakan. Berkat adanya *SQL* maka dari itu para *programmer* jaringan dan aplikasi tidak menemukan permasalahan yang berarti dalam mengintergrasikan aplikasi yang dibuat. *MySQL* merupakan sistem *database* yang cepat, *user MySQL* dapat menggunakan sistem dengan berbarengan. *MySQL* ialah salah satu perangkat lunak gratis yang bisa diunduh pada laman resminya. *MySQL* juga merupakan sebuah sistem manajemen *database*, relasional sistem *database* dan *software open source*. Jika *SQL* biasa disebut dengan istilah *SEQUEL* namu *MySQL* tidak disebut dengan *MY-SEQUEL* karena pencetusnya sendiri menyebutkan *MySQL* dengan istilah "*My Ess Que Ell*".(Sakur, 2004)

2.6 *Apache*

Apache adalah *software web server* yang terkenal yang dikembangkan pada tahun 1995. *Server Apache* telah dikembangkan oleh *Apache Software Foundation*, yang anggotanya terus menambahkan fungsionalitas baru yang bermanfaat, dengan tujuan menyediakan *platform server* yang sangat aman dan dapat diperluas yang memastikan pengiriman layanan HTTP sesuai dengan standar HTTP. Versi asli *Apache* ditulis untuk UNIX, tetapi saat ini versi yang berjalan di bawah OS/2, *Windows* dan *platform* lainnya. *Server Apache* menyediakan berbagai fitur *web server*, termasuk CGI, SSL, dan *domain* virtual. *Apache* sangat mendukung modul plug-in. Disebut *Apache* karena dikembangkan dari kode NCSA yang sudah ditambah berbagai *patch*, oleh karena itu dinamakan *server patchy* atau *server Apache*.(Cecep Kurnia Sastradipraja & Munawar, 2002)

2.6 Sistem *Voting*

Penulis juga telah melakukan studi pustaka dari beberapa penelitian sebelumnya yang membahas topik relevan sesuai apa yang diteliti oleh penulis. Dari studi pustaka yang dilakukan, penulis merangkum hasilnya.

Penelitian pada tahun 2022 oleh Nurul Chafid dan Herlina dengan topik "Implementasi Algoritma Kriptografi Klasik *Caesar* untuk Rancang Bangun Aplikasi *E-Voting* Berbasis Web. Pada penelitian ini penulis membuat aplikasi yang bertujuan memudahkan admin dalam mengontrol data hasil *voting*. Saran dari penelitian ini untuk peneliti selanjutnya adalah untuk menambahkan fitur ekspor kedalam bentuk PDF atau Excel.

Penelitian berjudul "Implementasi Algoritma *Caesar Chiper* pada Keamanan Data Sistem *E-Voting* Pemilihan Ketua Organisasi Kemahasiswaan" pada tahun 2019 oleh Husni Angriani dan Yeni Saharaeni yang memiliki tujuan untuk membantu proses perhitungan yang cepat dengan biaya minim dibandingkan dengan proses manual. Saran dari penelitian ini adalah bisa melakukan penggabungkan dua algoritma kriptografi pada penelitian selanjutnya untuk memberikan hasil baik, sehingga pola deskripsi tidak mudah terdeteksi.

Berikut perbandingan jurnal terkait dengan penelitian ini yang sudah disajikan kedalam bentuk tabel. Jurnal yang dijadikan referensi adalah yang yang membahas penelitian dengan menggunakan algoritma kriptografi *Caesar Chiper*, AES dan Kriptografi Klasik *Caesar*. Tahun terbit jurnal yang dirincikan pada tabel dibawah memiliki rentang waktu dari tahun 2018 sampai dengan tahun 2022.

Tabel 2. 1 Perbandingan Studi Pustaka dengan Penelitian Terkait

No.	Penulis	Judul	Tujuan	Metode	Saran
1	Nurul Chafid, Herlina Soffiana/2022	Impelementasi Algoritma Kriptografi Klasik *Caesar* untuk Rancang Bangun Aplikasi *E-*	Mempermudah admin dalam mengelola data hasil *voting*	Kriptografi Klasik *Caesar*	Bisa ditambahkan fitur ekspor excel untuk rekap data

No.	Penulis	Judul	Tujuan	Metode	Saran
		Voting Berbasis Web			
2	Radithya Pramuditha Yenadi, Fauziah, Deny Hidayatulla h/2020	Implementasi Metode *Caesar Cipher* dalam Penerapan	Pengambilan keputusan secara terbuka, mempercepat, menghemat dan mencegah kecurangan	*Caesar Chiper*	-
3	Muhammad Azmi Adhani, Radityo Adi Nugroho, Rudy Herteno, Muliadi, Friska Abadi/2021	Pemilihan Ketua dan Wakil Ketua BEM ULM Berbasis Elektronik	penghematan biaya, waktu serta meminimalisir penyebaran wabah COVID-19	AES	-
4	Uung Ungkawa, Dewi Rosmala, Helmy Fauzi/2021	Penerapan *Advance Encryption Standart* dalam Pengamanan Elektronik *Voting*	Proses penghitungan suara lebih cepat dan hemat biaya	AES	-
5	Muhammad Agreindra	Sistem *E-Voting* Berbasis	Mengamanka n data agar	*Caesar Chiper*	-

No.	Penulis	Judul	Tujuan	Metode	Saran
	Helmiawan, Dani Indra Juna, Billy Ramdhani/20xx	Web pada Pemilihan Abang None Jakarta	data yang diterima sesuai dengan yang dimasukan		
6	Husni Angriani, Yeni Saharaeni/2019	Implementasi Algoritma *Caesar Cipher* pada Keamanan Data Sistem *E-Voting* Pemilihan Ketua Organisasi Kemahasiswaan	Meminimalisir penyalah gunaan data hasil pemilihan	*Caesar Chiper*	Menggabungkan dua algoritma sehingga sulit untuk menemukan pola dekripsi
7	Intan Fitirani/2020	Implementasi Algoritma *Advanced Encryption Standard* (AES) pada Layanan SMS Desa	menambahkan keamanan data SMS pada sistem Layanan SMS Desa agar tidak disalahgunakan	AES	sistem dapat dikembangkan ke media online lain seperti telegram.
8	Nurhidayat Subagio, Wahyuni Eka Sari,	Perancangan Sistem *E-voting* berbasis Web untuk Ketua Himpunan	mudah dalam melakukan pemilhan dan waktu	-	diimplementasikan dengan teknologi android

No.	Penulis	Judul	Tujuan	Metode	Saran
	Yulianto/2020	Mahasiswa Teknologi RPL	menjadi lebih efesinsi		
9	Fitri Nuraeni, Yoga Handoko Agustin, Angga Eka Purnama/2020	Implementasi *Caesar Chiper* dan AES pada Pengamanan Data PBB	Mengamankan data pajak bumi dan bangunan	*Caesar Chiper* dan AES	Kunci untuk proses enkripsi dan deskripsi dibuat beragam
10	Risnaty Utami Marsa, Fitri Arnia, Ramzi Adriman/2018	Enkripsi dan Dekripsi Citra Menggunakan Modifikasi Algoritma *Vigenere Cipher*	Memodifikasi algoritma *Vigenere Cipher*	*Vigenere Cipher*	

Pada table 2.1 terdapat beberapa jurnal relevan yang menjadi referensi dalam penelitian ini. Dan dari beberapa jurnal tersebut terdapat saran-saran yang diberikan penulis tersebut.