

No.	Nama Peneliti	Judul Penelitian	Hasil
			Juga Waktu Enkripsi Dan Dekripsinya Dan Terdapat Karakter Tambahan Yaitu Karakter <i>Space</i> .
2	(Hariati et al., 2018a)	Kombinasi Algoritma <i>Playfair Cipher</i> Dengan Metode Zig-Zag Dalam Penyandian Teks	Dari Hasil Penelitian Ini Teknik Kriptografi Dengan Algoritmanya Dapat Merubah Teks Informasi Asli Menjadi Sandi-Sandi (Simbol-Simbol) Yang Sangat Sulit Ditemukan Korelasi Dan Makanya. Algoritma <i>Playfair Cipher</i> Melakukan Penyandian Teks Dengan Mensubstitusikan Masing-Masing Karakter Teks Dengan Karakter Yang Baru Sesuai Dengan Formulasinya, Sedangkan Metode Zig-Zag Akan Melakukan Transposisi Atau Pengacakan Posisi Karakter-Karakter Yang Dihasilkan Dari Proses Enkripsi <i>Playfair Cipher</i> .
3	(Hondro, 2020)	Modifikasi Platform Kunci Algoritma <i>Playfair</i> Untuk Meningkatkan Nilai Confusion Pada <i>Ciphertext</i>	Hasil Dari Penelitian Ini Adalah Dari Modifikasi Algoritma <i>Playfair</i> Dapat Diterapkan Pada Proses Enkripsi Sehingga Menghasilkan <i>Ciphertext</i> Yang Memiliki Nilai Confusion. Selain Itu Juga Dapat Diterapkan Pada Proses Dekripsi Sehingga Menghasilkan Plaintext Yang Dapat Dimengerti.
4	(Hariati et al., 2018b)	Kombinasi Algoritma <i>Playfair Cipher</i> Dengan Metode Zig-zag Dalam Penyandian Teks	Teknik kriptografi dengan algoritmanya dapat merubah teks informasi asli menjadi sandi-sandi (simbol-simbol) yang sangat sulit ditemukan korelasi dan makanya. Algoritma <i>playfair cipher</i> melakukan penyandian teks dengan mensubstitusikan masing-masing karakter teks dengan karakter yang baru sesuai dengan formulasinya, sedangkan metode zig-zag akan melakukan

No.	Nama Peneliti	Judul Penelitian	Hasil
			transposisi atau pengacakan posisi karakter-karakter yang dihasilkan dari proses enkripsi <i>playfair cipher</i>
5	(Eka, 2018)	Implementasi Keamanan Data Menggunakan Algoritma Vernam Cipher Dan <i>Playfair Cipher</i>	Masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu.dalam kesempatan ini penulis akan mencoba menjelaskan berbagai macam ancaman keamanan data dan cara mengatasi ancaman tersebut. Kriptografi dapat menjadi jawaban dari masalah tersebut.

Penelitian ini memiliki tinjauan pustaka dari beberapa jurnal atau penelitian yang memiliki kesamaan atau keterkaitan. **Pada Tabel.2** terdapat beberapa penelitian atau jurnal terkait dengan penelitian ini yaitu jurnal tentang implementasi keamanan data menggunakan metode kriptografi. Perbedaan penelitian ini dengan penelitian-penelitian terkait terletak pada penggunaan algoritma yang digunakan pada penelitian, algoritma yang digunakan pada penelitian terkait kombinasi antar algoritma *zig-zag* dan *playfair chipper*, algoritma *venam chipper* dan *playfair chipper*, modifikasi *playfair chipper* untuk mengamankan pesan text, sedangkan pada penelitian ini peneliti menggunakan algoritma *playfair chipper* untuk mengamankan data-data yang dianggap penting di SMAN 3 Tana Toraja.

H. Landasan Teori

Bagian ini memberikan beberapa konsep teori yang mendukung penelitian. landasan teori yang digunakan serta dijadikan sebagai acuan dalam penelitian ini antara lain;

1. Kriptografi

Kriptografi merupakan ilmu yang menerapkan teknik keamanan mengenai penyandian (enkripsi) dimana naskah/pesan asli yang disebut *plaintext* diacak dengan menggunakan kunci yang telah ditentukan sehingga menghasilkan naskah/pesan yang acak dan tidak dapat dipahami makna/artinya objek pesan/naskah ini disebut dengan istilah *ciphertext* (Hondro, 2020).

Hal-hal yang harus tercapai dalam menggunakan kriptografi untuk mengamankan data adalah aspek kerahasiaan artinya informasi harus benar-benar terjaga aksesnya dari pihak yang tidak berwenang, integritas data adalah aspek yang bertujuan untuk mencegah terjadinya perubahan informasi oleh pihak-pihak yang tidak berwenang, autentikasi yang berhubungan dengan pemeriksaan hak akses dan yang terakhir adalah nir-penyangkalan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku (Hariati, dkk, 2018).

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data atau informasi (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*). Metode dari enkripsi adalah fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Metode yang digunakan menentukan

kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika (Susanti, 2019).

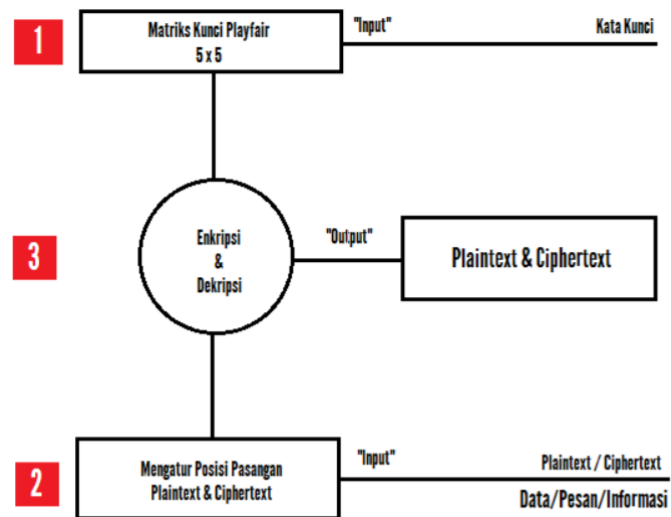
2. *Playfair Cipher*

Playfair Cipher ditemukan oleh *Sir Charles Wheatstone* (1802-1875) pada tahun 1854, dan dipopulerkan oleh *Baron Lyon Playfair* (1819-1898), yang namanya diabadikan untuk algoritma ini. Meskipun algoritma *Playfair* ini sudah tidak aman untuk kegunaan dunia saat ini, *Playfair cipher* banyak digunakan dan cukup efektif pada jamannya. *Playfair cipher* pertama kali digunakan oleh tentara Inggris pada perang *Boer* dan masih digunakan pada Perang Dunia I (Solihin et al., 2017).

Playfair Cipher merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam polygram cipher, dimana *plainteks* diubah menjadi bentuk poligram dan proses enkripsi dekripsi dilakukan untuk poligram tersebut. Kunci kriptografinya adalah 25 buah huruf yang disusun di dalam bujursangkar 5x5 dengan menghilangkan huruf J dari abjad. Kemungkinan kuncinya adalah 25!. Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam. Basis keenam merupakan baris pertama, sementara kolom keenam berisi kolom pertama. Pada umumnya, kunci yang digunakan adalah serangkaian kata yang mudah dimengerti (Syahputra, 2018).

Algoritma *Playfair* bekerja dengan tiga tahap utama yaitu membuat bujursangkar/matriks kunci, proses mengatur pesan, proses enkripsi/dekripsi

lebih jelas dapat dilihat model gambarnya pada Gambar1(Skema Kerja *Playfair Cipher*) (Hondro, 2020):



Gambar 1. Skema Kerja *Playfair Cipher*

3. Database

Database adalah kumpulan dari catatan-catatan, atau potongan dari pengetahuan. Sebuah database memiliki penjelasan terstruktur dari jenis fakta yang tersimpan di dalamnya: penjelasan ini disebut skema. Skema menggambarkan objek yang diwakili suatu database, dan hubungan di antara objek tersebut. Ada banyak cara untuk mengorganisasi skema, atau memodelkan struktur database: ini dikenal sebagai database model atau model data.

Model yang umum digunakan sekarang adalah model relasional, yang menurut istilah yaitu mewakili semua informasi dalam bentuk tabel-tabel yang saling berhubungan dimana setiap tabel terdiri dari baris dan kolom (definisi yang sebenarnya menggunakan terminologi matematika). Dalam model ini,

hubungan antar tabel diwakili dengan menggunakan nilai yang sama antar tabel. Model yang lain seperti model hierarkis dan model jaringan menggunakan cara yang lebih eksplisit untuk mewakili hubungan antar tabel.

Konsep dasar dari basis data ialah kumpulan dari sebuah catatan atau sebuah potongan dari pengetahuan. Sebuah basis data memiliki penjelasan testruktur dari jenis fakta yang tersimpan di dalamnya, penjelasan tersebut dengan skema. Skema menggambarkan sebuah objek yang diwakili suatu basis data dan memiliki hubungan diantara objek tersebut. Ada banyak cara untuk mengorganisasi skema atau memodelkan struktur basis data, ini dikenal sebagai model basis data atau model data. Biasanya model yang umum digunakan sekarang ialah model relasional yang istilahnya layman mewakili semua informasi dalam bentuk tabel-tabel yang saling berhubungan dimana setiap tabel terdiri dari baris dan kolom (definisi yang sebenarnya menggunakan terminologi matematika). Dalam model ini hubungan antar tabel diwakili dengan menggunakan nilai yang sama antar tabel. Model yang lain seperti model hierarkis dan model jaringan menggunakan cara yang lebih eksplisit untuk mewakili hubungan antar tabel.(Pahlevi et al., 2018)

4. PHP

PHP (Hypertext Preprocessor) yaitu bahasa pemrograman *web serverside* yang bersifat *open source*. PHP merupakan script yang digunakan untuk membuat halaman *website* yang dinamis, dinamis berarti halaman yang akan ditampilkan dibuat saat halaman itu diminta oleh *client*. Mekanisme ini

menyebabkan informasi yang diterima *client* selalu yang terbaru/*up to date*. Semua script PHP dieksekusi pada *server* dimana script tersebut dijalankan

PHP adalah bahasa pemrograman untuk dijalankan melalui halaman web, umumnya digunakan untuk mengolah informasi diinternet. Sedangkan dalam pengertian lain PHP adalah singkatan dari *Hypertext Preprocessor* yaitu bahasa pemrograman *webserver-side* yang bersifat *open source* atau gratis. PHP merupakan script yang menyatu dengan HTML dan berada pada server (Didi Susianto, 2020)

I. Metodologi Penelitian

1. Tahapan Penelitian

a. Pengumpulan Data

Pengumpulan data-data dan informasi yang dibutuhkan akan dilakukan dengan cara mengamati secara langsung permasalahan pada sistem yang telah ada. Selain itu, penulis juga melakukan pertemuan dan wawancara kepada pihak-pihak yang nantinya akan berhubungan dengan sistem yang akan dirancang.

b. Analisis Sistem

Pada tahap analisis sistem, penulis akan menganalisis bagaimana membangun sebuah aplikasi nilai berbasis web menggunakan metode kriptografi. Tujuan utamanya adalah untuk memahami kesalahan yang ada pada aplikasi nilai sebelumnya.

c. Perancangan Sistem

Sistem yang akan dibangun adalah aplikasi nilai siswa berbasis web dengan menggunakan bahasa pemrograman PHP. Sistem ini diharapkan dapat membantu mengatasi kekurangan-kekurangan yang ada pada sistem sebelumnya.

d. Implementasi

Tahap implementasi dilakukan setelah tahap perancangan sistem. Tahapan ini masuk pada proses menulis kode program untuk membangun sistem sesuai perancangan yang dilakukan.

e. Pengujian Aplikasi

Pengujian terhadap sistem dilaksanakan setelah sebuah program aplikasi selesai dibuat. Pengujian dilakukan sebagai tolak ukur bahwa perangkat lunak yang telah dibuat tidak mempunyai kesalahan, dengan melakukan pengujian kesalahan pada perangkat lunak dapat diperbaiki sehingga perangkat lunak yang dibuat dapat sesuai dengan kebutuhan dan tujuan pembuatannya. Pendekatan pengujian yang akan dilakukan adalah *black box testing*.

2. Instrumen Penelitian

Instrumen penelitian adalah alat bantu yang dipilih dalam kegiatannya agar sistematis dan mempermudah peneliti selama melakukan penelitian. Instrumen ini terbagi menjadi dua yaitu:

a. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan adalah:

- 1) Laptop Asus A407UA
- 2) *Processor Intel® Core™ i3*
- 3) RAM 4,00 GB

b. Perangkat Lunak (*Software*)

Perangkat lunak atau *software* yang digunakan adalah:

- 1) Microsoft Windows 10 Professional 64-bit, sebagai Sistem Operasi.
- 2) JDK versi 1.8.0_161.
- 3) Netbeans

3. Lokasi Penelitian

Lokasi penelitian ini dilakukan pada Sekolah SMAN 3 Tana Toraja, Rante Kalua', Mengkendek, Kabupaten Tana Toraja. Penelitian ini dilakukan kurang lebih 5 bulan terhitung sejak Februari 2021 sampai Juni 2021

4. Metode Penelitian

a. Pengumpulan Data

Pengumpulan data-data dan informasi yang dibutuhkan akan dilakukan dengan cara wawancara langsung kepada pihak yang tau banyak mengenai sistem aplikasi nilai SMAN 3 TANA TORAJA. Data dan informasi yang dibutuhkan adalah keamanan data-data siswa dan kerahasiaanya .

b. Analisis Sistem

Pada tahap analisis sistem, penulis akan menganalisis bagaimana merancang sebuah aplikasi nilai siswa dengan menggunakan metode

kriptografi untuk mengamankan data-data siswa yang di anggap harus dijaga kerahasiaanya, dengan data informasi yang bersumber dari proses wawancara sebelumnya.

c. Perancangan Sistem

1. Perancangan Antarmuka Sistem

Sistem yang diusulkan oleh penulis memiliki beberapa perancangan halaman sebagai berikut.

a) Halaman Login admin.

Administrator dalam hal ini adalah Staf Tata Usaha. Admin dapat menambahkan, menyimpan, memperbaharui dan menghapus pengumuman, data user, data guru, siswa, pelajaran, kelas, kelas siswa, nilai kelas dan laporan.

Header	
Gambar	LOGIN ADMIN
	<input type="text" value="Username"/>
	<input type="text" value="Password"/>
	<input type="button" value="LOGIN"/>
Footer	

Gambar 2. Login administrator

b) Halaman Utama Administrator ini terdapat beberapa menu-menu yang terdiri dari home, data user, data guru, data siswa, data kelas, nilai kelas, laporan, dan logout.

Header	
<ul style="list-style-type: none"> • Home • Data User • Data Guru • Data Siswa • Data Kelas • Nilai Kelas • Laporan • Logout 	Content
Footer	

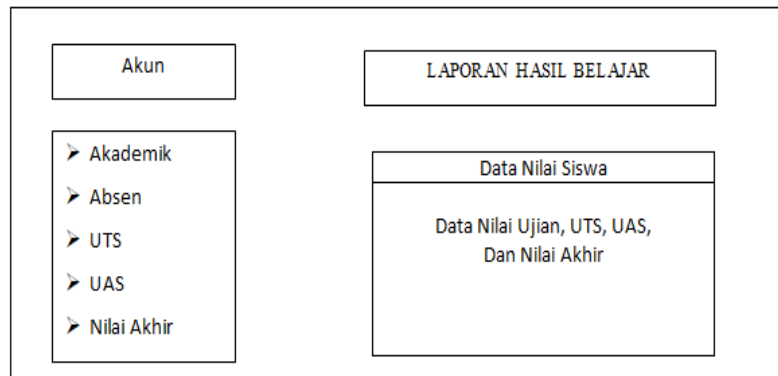
Gambar 3. Menu Utama Administrator

- c) Halaman utama administrator di bagian menu data guru admin dapat menambahkan data guru dan dapat menghapus data .

Header						
<ul style="list-style-type: none">• Home• Data User• Data Guru• Data Siswa• Data Kelas• Nilai Kelas• Laporan• Logout	Data Guru					
	+ Add Data					
	No	Kode	Nlp	Nama Guru	Mata Pelajaran	Jenis Kelamin
	9.	xx	xxxx	xxxx	xxxxx	x
	9.	xx	xxxx	xxxx	xxxxx	x
Footer						

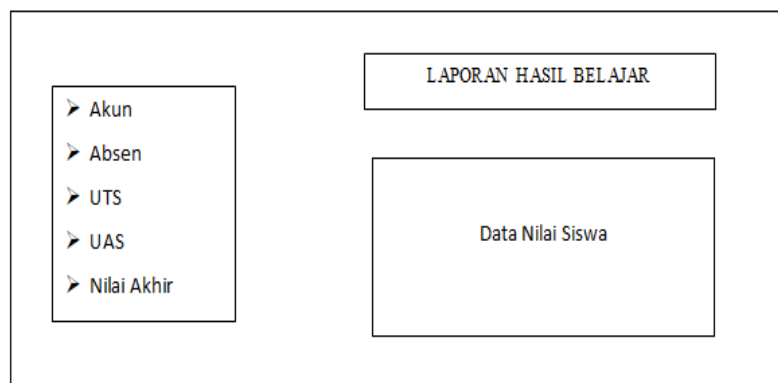
Gambar 4. Menu Utama Administrator

- d) Menu utama Siswa ada terdapat beberapa menu-menu yang dapat di akses oleh siswa, siswa dapat melihat data pribadi, data pelajaran, data guru, dan rapor.



Gambar 5. Menu Utama Siswa

- e) Halaman Menu utama orang tua siswa yaitu Orang Tua memiliki akses untuk login dan melihat bukti ujian siswa, rekapitulasi absen dan kehadiran, serta melihat ujian dan nilai akhir semester.



Gambar 6. Menu Utama Orang tua Siswa

Sistem yang akan dibangun adalah aplikasi nilai siswa berbasis *website* menggunakan bahasa pemrograman PHP. Sistem dibangun dengan fitur utama berupa halaman login untuk admin, halaman utama siswa dan orang tua siswa.

d. Implementasi

Tahap implementasi dilakukan setelah tahap perancangan sistem. Tahapan ini masuk pada proses menulis kode program untuk membangun sistem sesuai perancangan yang dilakukan.

e. Pengujian Aplikasi

Aplikasi diuji untuk mengetahui keberhasilan penerapan metode kriptografi dalam mengamankan data-data siswa dengan melihat output yang dihasilkan oleh sistem sesuai dengan yang dihadapkan.