

Implementasi Metode Zig-Zag Cipher Pada Script Php

Implementation Of The Zig-Zag Cipher Method In Php Script

Indah Mutiara^{a,1}, Lili Tanti^{b,2}

^aProgram Studi Informatika UPU, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^b Dosen Program Studi Informatika UPU, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia
indahmutiara031000@gmail.com¹, lilitanti82@gmail.com²

ABSTRAK

Script PHP dapat dilihat langsung di jendela cybersurfer oleh penjelajah internet. Hal ini memungkinkan peretas atau pencuri informasi untuk meniru atau menghargai isi skrip PHP untuk mengungkapkan informasi penting dalam database. Oleh karena itu diperlukan pengamanan agar script PHP tidak dapat dilihat oleh orang yang tidak diinginkan. Caranya adalah dengan menerapkan sistem kriptografi pada skrip PHP. Dengan melakukan cracking script PHP maka seseorang yang melihat isi script PHP tidak akan cocok untuk melihat isi script PHP yang sebenarnya. Untuk itu penulis merekomendasikan sistem Zigzag sebagai algoritma garbling PHP Script. Ketika penggunaannya semakin luas, hal ini menimbulkan kejahatan yang disebut "kejahatan dunia maya". Kejahatan-kejahatan ini termasuk mencuri kaki kartu kredit, memblokir data tertentu seseorang seperti alamat pengiriman, atau memanipulasi informasi dari pelari situs web dengan tujuan mendapatkan apa yang mereka inginkan. Untuk mendesain sebuah website, seorang programmer dapat menggunakan beberapa bahasa pemrograman, salah satunya adalah PHP (Hypertext Preprocessor). Saat ini PHP digunakan di lebih dari 22 juta situs web dan PHP semakin tidak stabil dan lebih dapat diperluas dibandingkan kinerja pendahulunya. Website yang menggunakan bahasa pemrograman PHP antara lain bisnis, teknologi, belanja, berita, pendidikan, sosial, hiburan, dll. Namun software PHP harus didistribusikan dalam bentuk sumber, sehingga memiliki beberapa kegagalan dan celah keamanan. Salah satu kelemahannya adalah skrip dapat dengan lancar disalin, diubah, atau digunakan secara tidak lengkap di perangkat lunak lain tanpa pemberitahuan. Selain itu, skrip yang tidak terenkripsi membuat perangkat lunak menjadi sangat rentan, karena skrip dapat mengungkap beberapa kelemahan perangkat lunak. Oleh karena itu diperlukan suatu hasil yang dapat mengamankan skrip operasi PHP yang akan didistribusikan.

Kata Kunci : Zig Zag Cipher, Script, PHP, Android Studi

ABSTRACT

PHP scripts can be seen directly in the browser window by internet explorers. This allows hackers or information thieves to imitate or extract the contents of PHP scripts to reveal important information in the database. Therefore, security is needed so that the PHP script cannot be seen by unwanted people. The way to do this is to apply a cryptographic method to PHP script. By encrypting the PHP script, someone who views the contents of the PHP script will not be able to see the actual contents of the PHP script. For this reason, the author recommends the Zigzag method as a PHP Script encoding algorithm. As its use becomes more widespread, it gives rise to a crime called "cybercrime". These crimes include stealing credit card PINs, intercepting someone's personal data such as email addresses, or manipulating information from a website page with the aim of getting what they want. To design a website, a programmer can use several programming languages, one of which is PHP (Hypertext Preprocessor). Currently PHP is used on more than 22 million websites and PHP is increasingly stable and more extensible than its predecessor versions. Websites that use the PHP programming language include business, technology, shopping, news, education, social, entertainment, etc. However, PHP software must be distributed in source form, so it has several shortcomings and security gaps. One of these disadvantages is that scripts can easily be copied, changed, or partially used in other software without notification. In addition, unencrypted scripts make the software being built very vulnerable, because scripts can reveal some weaknesses of the software. That's why there is a need for a solution that can secure PHP application scripts that will be distributed.

Keywords : Zig Zag Cipher, Script, PHP, Android Studio

1. PENDAHULUAN

Kemajuan kearifan dan teknologi saat ini mendorong setiap orang/eksistensi, instansi atau perusahaan, baik pemerintah maupun swasta, untuk selalu menemukan dan memanfaatkan teknologi sebagai alat untuk membantu menjalankan tugas setiap yang ada di dalamnya, serta membantu dalam permasalahan pekerjaan. yang muncul. menghadap. Pengoperasian sistem informasi berbasis komputer dirasa lebih efektif dan efektif dibandingkan dengan sistem konvensional atau buatan sendiri(1). Sistem informasi berbasis komputer juga merupakan strategi keunggulan kompetitif dan merupakan pilihan tepat untuk menyempurnakan pelayanan. Jebakan terhadap keamanan komunikasi dapat terjadi kapan saja. data non-publik yang akan ditransfer memerlukan keamanan agar tidak dapat disalahgunakan oleh pihak lain. Data yang ingin disampaikan memerlukan pengamanan sehingga hanya dapat digunakan oleh donatur yang berwenang (2)

Dalam eksplorasi ini digunakan pembangkitan krusial dengan menggunakan algoritma LUC. Kriptosistem mongrel adalah suatu sistem untuk mengunci algoritma dengan harmoni simetris dan asimetris yang digunakan untuk mengamankan harmoni algoritma. Algoritma ini digunakan untuk mengkodekan buku teks biasa sedangkan algoritma RSA-LUC digunakan untuk mengkodekan kunci break-swerve. Hasil dari eksplorasi ini adalah semakin panjang jumlah karakter maka semakin lama pula proses yang diperlukan untuk proses enkripsi pada baris-baris buku teks (12)

Android Studio adalah Lingkungan Pengembangan Terpadu (IDE) untuk pengembangan operasi Android, yang didasarkan pada IntelliJ IDEA. Konsepsi Android Inc diduga membangkitkan minat Google untuk mempertahankannya. Pada bulan Agustus 2005, Android Inc akhirnya diakuisisi oleh GoogleInc. semua saham dibeli oleh Google.(13

MySQL (My Structure Query Language) merupakan program pembuatan database yang bersifat Open Source, artinya semua orang dapat menggunakannya dan dapat berjalan di semua platform baik Windows maupun Linux. MySQL juga merupakan perangkat lunak sistem operasi database SQL yang berjaringan sehingga dapat digunakan untuk operasi multi-user(14)

PHP atau kependekan dari Hypertext Preprocessor adalah bahasa pemrograman open source yang sangat cocok atau khusus untuk pengembangan web dan dapat dituangkan dalam tesis HTML(15)

2. METODE

Berikut adalah alir diagram metode penelitian yang digunakan dalam penulisan proposal ini :

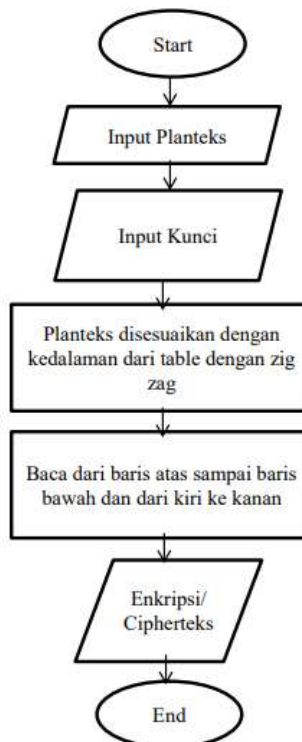


Gambar 1. Diagram Alir Metodologi Penelitian

3. HASIL DAN PEMBAHASAN

A. Pembahasan

Bagian flowchart enkripsi akan menggambarkan dan menjelaskan cara mengenkripsi pada program atau sistem, berikut ini adalah flowchart enkripsi.

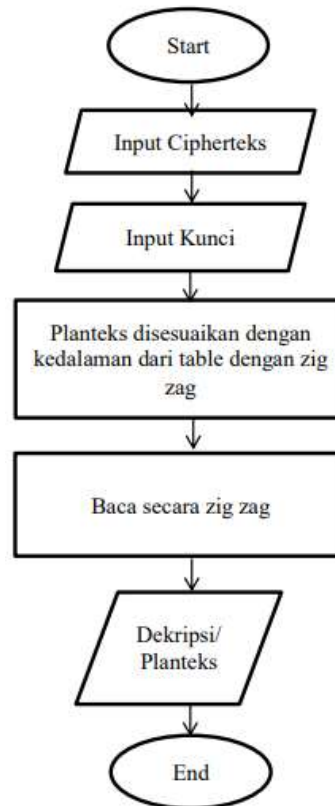


Gambar 2. Flowchart enkripsi

Gambar 2 menunjukkan alur pada saat mengenkripsi. gambar yang diatas menunjukkan bahwa proses enkripsi dimulai dengan menginput planteks dan Start Input Planteks Planteks disesuaikan dengan

kedalaman dari table dengan zig zag Enkripsi/ Cipherteks End Input Kunci Baca dari baris atas sampai baris bawah dan dari kiri ke kanan 33 juga kunci atau kedalaman, kemudian planteks akan disesuaikan dengan kunci ataupun kedalaman yang tadi diinputkan.

Flowchart dekripsi akan menjelaskan dan juga menggambarkan bagaimana proses program pada saat mengdekripsikan kalimat atau cipherteks



Gambar 3. Flowchart dekripsi

Gambar 3 menunjukkan alur pada saat mengdekripsi. gambar yang diatas menunjukan bahwa proses dekripsi dimulai dengan menginput Cipherteks yang didapat dan juga kunci yang sesuai dengan padasaat enkripsi, kemudian cipherteks akan disesuaikan dengan kunci yang sudah di tentukan dengan pengguna yang mengenkripsi.

Contoh kasus

Berikut ini akan diuraikan contoh penyandian teks berdasarkan algoritma zigzag ini. Berikut adalah contoh perhitungan sederhana menggunakan Metode Zig-Zag Cipher untuk plainteks dengan kunci (key) 3:

1) Validasi Data

```
<!DOCTYPE html>
```

```
<html>
```

```
<body> <h1>Halaman HTML</h1>
```

```
<?php echo "Halo dunia!"; ?>
```

```
</body>
```

```
</html>
```

Langkah 1: Membuat Zig-Zag Pattern

<				L				o				<				H				a						L
	H		M		\n		b		d		>		h		>		a		m		n				T	
		T				<				y				1					l					H		

<				
	h		>	
		1		

<			p				h				a				d				a				>
	?		h				c		o		"		l			u		i		!		?	
		p					e						o				n					;	

<				d				<				>
	/		o		y		\n		h		l	
		b					>			m		

Langkah 2: Membaca dari Zig-Zag Pattern berdasarkan kunci (key) 3

h				o				l	
	e		l		w		r		d
		l				o			

maka Ciphertext = <Lo<HaL<HM\nbd>h>amnTh>T<y1lH1<phada>?hc0"lui!?peon;<d<>/oy\nhlb>m

Untuk mengembalikan pesan yang telah disandikan maka dilakukan proses dekripsi

Proses Dekripsi Zig-zag Cipher (ZzC):

Ciphertext =

<Lo<HaL<HM\nbd>h>amnTh>T<y1lH1<phada>?hc0"lui!?peon;<d<>/oy\nhlb>m

Deretan karakter pada ciphertext akan dibagi menjadi 3 bagian dan diisi ke dalam kolom dengan pola Zig-Zag sesuai urutan baris pada pembagian tersebut. Berikut ini proses dekripsi Zig-Zag Cipher :

< (1)				L (2)				o(3)				<(4)			
	H(9)		M(10)		\n(11)		b(12)		d(13)		>(14)		h(16)		>(16)
		T(20)					<(21)				y(22)				1(23)

H(5)				a(6)				L(7)	<(8)		
	a(17)		m(18)		n(19)		T(20)		h(21)		>(22)
		l(24)					H(25)				1(23)

<(24)				p(25)				h(26)				a(27)		
	?(31)		h(32)				c(33)		o(34)		"(35)		l(36)	
		p(41)					e(42)							o(43)

d(28)				a(29)				>(30)
	u(37)		i(38)		!(39)		?(40)	
		n(44)				;(45)		

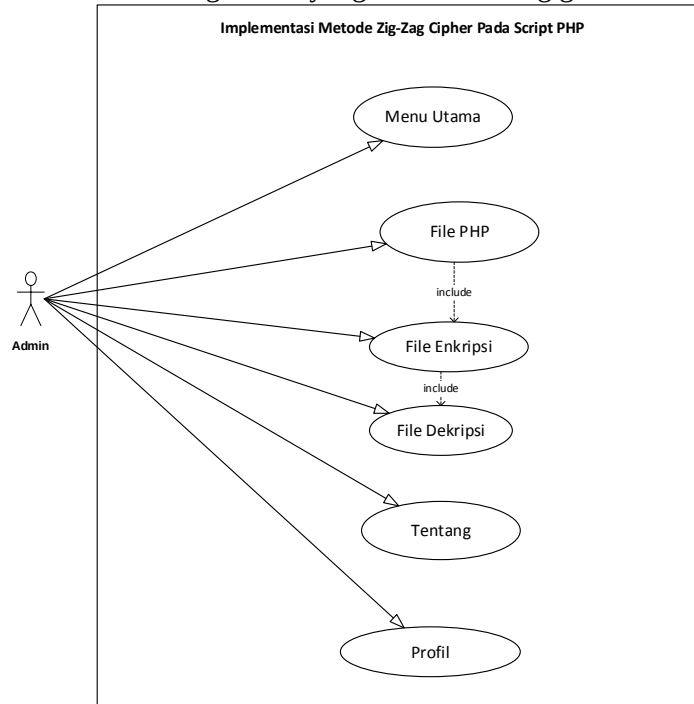
<(46)				d(47)				<(48)				>(49)
-------	--	--	--	-------	--	--	--	-------	--	--	--	-------

	/ (50)		o (51)		y (52)		\n (53)		h (54)		l (55)	
		b (56)				> (57)				m (58)		

<(1) H(9) T(20) M(10) L(2) \n(11) <(21) b(12) o(3) d(13) y(22) >(14) <(4)

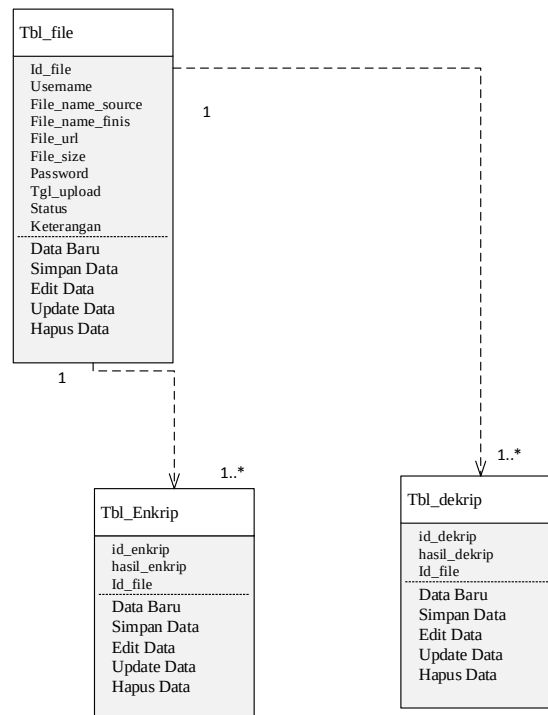
B. DESAIN SISTEM

Perilaku beserta tugas-tugas dari tiap–tiap elemen maupun aktor yang terlibat dalam sistem yang akan dirancang, akan digambarkan dalam diagram *use case* yang bertujuan untuk memberikan gambaran secara umum tentang sistem yang akan dirancang gambar 4 sebagai berikut:



Gambar 4. *Use Case Diagram* Implementasi Metode Zig-Zag Cipher

Pada Script PHP Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar III.2 :



Gambar 5. Class Diagram Implementasi Metode Zig-Zag Cipher Pada Script PHP

C. Hasil

1) Tampilan Form Utama

Form utama merupakan *interface* program kriptografi secara keseluruhan, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* utama. Dalam *form* utama terdapat beberapa menu yaitu, menu *file* dan menu *program*. Untuk lebih jelasnya tampilan *form* utama dapat dilihat pada Gambar 6 dibawah ini.



Gambar 6.. Tampilan Form Utama

2) Tampilan *Form Data Enkripsi*

Form enkripsi ini berfungsi untuk merubah isi data *file* dalam bentuk *chipertext*, sehingga isi *plaintext* tidak dapat dikenali isi datanya dan hanya bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data enkripsi seperti memasukkan data *file PHP*, menyimpan hasil enkripsi (*chipertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data enkripsi dapat dilihat pada gambar 7 berikut ini:

Gambar 7. Tampilan *Form Data Enkripsi*

3) Tampilan *Form Data Upload File Enkripsi*

Form enkripsi ini berfungsi untuk merubah isi data *file* dalam bentuk *chipertext*, sehingga isi *plaintext* tidak dapat dikenali isi datanya dan hanya bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data enkripsi seperti memasukkan data *file PHP*, menyimpan hasil enkripsi (*chipertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data enkripsi dapat dilihat pada gambar 8 berikut ini:

Gambar 8. Tampilan *Form Data Upload Enkripsi*

4) Tampilan *Form Dekripsi*

Form data dekripsi ini berfungsi untuk merubah isi data *chipertext* dalam bentuk *plaintext*, sehingga isi *chipertext* dapat dikenali kembali isi datanya dan bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data dekripsi, seperti memasukkan atau membuka data teks (*chipertext*), menyimpan hasil dekripsi (*plaintext*), dan keluar dari *form* dekripsi.

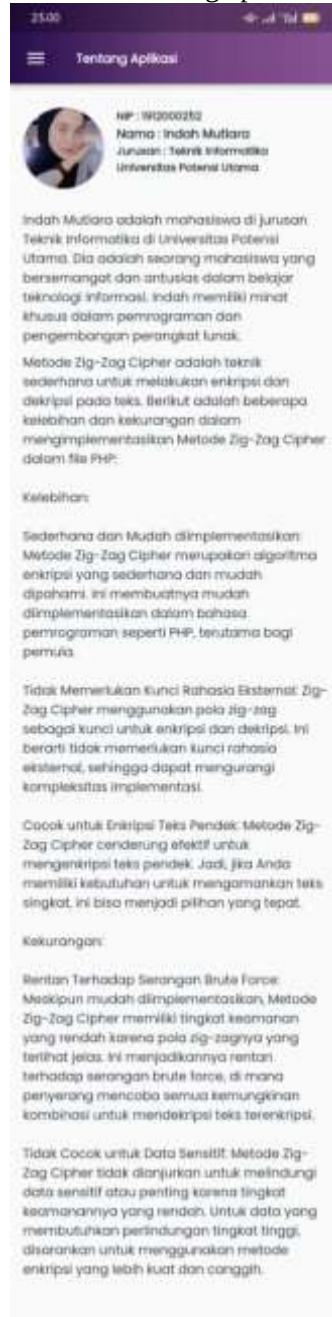
Gambar 9. Tampilan *Form Dekripsi*

5) Tampilan *Form Upload File Dekripsi*

Form data dekripsi ini berfungsi untuk merubah isi data *chipertext* dalam bentuk *plaintext*, sehingga isi *chipertext* dapat dikenali kembali isi datanya dan bisa dibuka dengan menggunakan kunci yang diberikan oleh *user* terhadap sistem. Ada beberapa hal yang bisa dilakukan didalam *form* data dekripsi, seperti memasukkan atau membuka data teks (*chipertext*), menyimpan hasil dekripsi (*plaintext*), dan keluar dari *form* dekripsi.

Gambar 10. Tampilan *Form* Upload File Dekripsi6) Tampilan *Form* Tentang

Form tentang berfungsi untuk melihat tentang aplikasi, dapat dilihat sebagai berikut ini:

Gambar 11 Tampilan *Form* Tentang7) Tampilan *Form* Akun

Form tentang berfungsi untuk melihat tentang akun pengguna, dapat dilihat sebagai berikut ini:



Gambar 12. Tampilan *Form Akun*

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan, dapat disimpulkan Aplikasi Telah dibangun dan dapat memanipulasi data file *Script PHP* dan terhadap isi suatu *file Script PHP* dengan system penyandian Aplikasi algoritma *Zig zag*. Sistem yang dibangun sudah mampu melakukan enkripsi dan dekripsi terhadap data Sehingga dapat Melindungi data-data P Dengan Menggunakan Metode *Zig zag*. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan mudah digunakan oleh *user*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian Penelitian ini.

REFERENSI

- [1]Fitriyani A, Handayani R, & Widanengsih E. (2020). Sistem Pendukung Keputusan Pemilihan Jurusan Pada SMK YMIK Joglo Jakarta Barat Menggunakan Metode Simple Additive Weigting (SAW). *Jtksi*, 03(01), 11–19.
- [2]Hariati, A., Hardiyanti, K., & Putri, W. E. (2018). Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks. *Sinkron*, 2(2), 13–17. <https://jurnal.polgan.ac.id/index.php/sinkron/index>
- [3]Janis, J. W., Mamahit, D. J., Sugiarto, B. A., Rumagit, A. M., Elektro, T., Sam, U., & Manado, R. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. *Jurnal Teknik Informatika*, 15(1), 1–12. <https://doi.org/10.35793/jti.15.1.2020.29023>
- [4]Lubis, R. S., Tulus, & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig- Zag dalam Hybrid Crypto Sistem. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, 6(2), 185–189.
- [5]Marpang, R., & Informasi, T. (2022). *PENYIMPANAN DATA PRIBADI DENGAN METODE*. 2(11), 1–14.
- [6]Muharromin, M., Informatika, J. T., & Darma, U. B. (n.d.). *Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache*. 393–402.
- [7]Pamungkas, P. G., & Muhammad, A. H. (2022). Modifikasi Algoritma Kriptografi Caesar Chiper pada Deretan Simbol dan Huruf di Smartphone dan Laptop. *Journal of Information Technology*, 2(1), 1–5.

<https://doi.org/10.46229/jifotech.v2i1.234>

- [8]Perbawa, K. A. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game Penerapan Algoritma Linear Congruential Generator (LCG) dalam Game Edukasi Matematika Berbasis Android. *Jurnal Komputer, Informasi Dan Teknologi*, 2(1), 47–56.
- [9]Ruing, M. O. I., & Ujianto, E. I. H. (2020). *Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) Dan Metode Steganografi Lsb Untuk Mengamankan Pesan Ke Dalam Citra Digital*. 1–8. <http://eprints.uty.ac.id/4888/>
- [10]Setiaji, A. (2020). RANCANG BANGUN APLIKASI PEMESANAN DESAIN JERSEY BERBASIS ANDROID DENGAN MENGGUNAKAN TEKNOLOGI FIREBASE (Studi Kasus : Konfeksi Minister). *Jurnal Sistem Informasi Dan Sains Teknologi*, 2(2). <https://doi.org/10.31326/sistek.v2i2.664>
- [11]Suheri, A. (2017). Keamanan File Dengan Teknik Zig-zag dan Huffman. *Media Jurnal Informatika*, 9(2), 78–83. <https://jurnal.unsur.ac.id/mjinformatika/article/view/450>
- [12]Suparman, B. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebas Java Desktop. *OKTAL: Jurnal Ilmu Komputer Dan Sains*, 1(07), 808–817. <https://journal.mediapublikasi.id/index.php/oktal/article/view/777%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/777/304>
- [13] Alfina, O., & Harahap, F. (2019). Pemodelan Uml Sistem Pendukung Keputusan Dalam Menentukan Siswa Siswa Tunagrahita. *Methomika : Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 3(2), 143–150.
- [14] Amarta Sholehuddin, M. D., Auliasari, K., & Faisol, A. (2021). Pengembangan Sistem Ujian Online Minat Dan Bakat Siswa Smk Pada Smk Islam Batu. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 5(2), 534–540. <https://doi.org/10.36040/jati.v5i2.3723>
- [15] Anwar, S., Efendi, Y., Rustam, R., Krs, P., Wahana, A., Self, W. M., Kartu, B., Pengisian, D. A. N., Studi, R., Amik, K. R. S., Berbasis, W., & Diri, W. E. B. (2016). *MAHASISWA BARU DAN PENGISIAN KARTU RENCANA STUDI (KRS) AMIK WAHANA MANDIRI BERBASIS WEB MOBILE*. 9(1), 73–98.