

## Rancang Bangun Website Kriptografi Untuk Pengamanan File Gambar Digital

Ferdy Febriyanto <sup>[1]</sup>

Sistem Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam  
Universitas Tanjungpura  
[ferdyf@sisfo.untan.ac.id](mailto:ferdyf@sisfo.untan.ac.id)

### INFO ARTIKEL

**Diajukan :**

17 November 2022

**Diterima :**

29 November 2022

**Diterbitkan:**

7 Desember 2022

**Kata Kunci :**

kriptografi, enkripsi, deskripsi,  
base64, gambar

### INTISARI

Pengamanan data digital merupakan suatu tindakan penting yang wajib diperhatikan oleh pemiliknya. Terutama di era serba digital sekarang dimana Indonesia mulai mengadopsi konsep *Society 5.0*. Yang mana pada konsep ini banyak bermunculan inovasi teknologi diberbagai bidang kehidupan yang terhubung melalui *internet (Internet of Things)*, sehingga tidak mengherankan ada banyak data pengguna yang bersebaran di dunia maya. Salah satu data digital yang sangat sering disimpan ataupun disebarakan pengguna pada dunia maya adalah file foto dalam bentuk gambar digital. Banyak pengguna yang kurang menyadari bahwa menyimpan gambar digital tersebut pada suatu media di dunia maya belum 100% aman. Hal ini dapat dilihat dari banyak kasus terjadinya pencurian ataupun penyebaran gambar digital khususnya yang bersifat penting atau *private* oleh orang yang tidak bertanggung jawab, sehingga memberikan dampak materil maupun moril bagi pemilik aslinya. Berdasarkan permasalahan tersebut, peneliti mencoba untuk membuat suatu sistem yang dapat membantu mengamankan gambar digital dengan metode kriptografi. Metode ini akan mengubah file gambar digital menjadi bentuk teks terenkripsi (*ciphertext*) yang diproses dengan algoritma *Base64*, sehingga orang lain tidak bisa melihat gambar dari file tersebut. Dari hasil pengujian terhadap lima (5) file gambar digital yang berbeda, semuanya berhasil di enkripsi kedalam bentuk file *ciphertext* walaupun ukuran file menjadi lebih besar dibandingkan file aslinya. Tetapi ketika dilakukan proses deskripsi (*ciphertext* menjadi file gambar), ukuran file menjadi seperti semula dan tidak ada penurunan kualitas file gambar.

### I. PENDAHULUAN

Indonesia sekarang ini mulai mengadopsi konsep masyarakat 5.0 atau yang dikenal dengan istilah *Society 5.0* dimana bentuk kegiatan ini berfokus pada lingkungan masyarakat yang terpusat pada aktivitas manusia yang berbasis IT (Wijayanti et al., 2022). Penerapan masyarakat 5.0 khususnya di Indonesia mengakibatkan banyak bermunculan inovasi teknologi diberbagai bidang kehidupan yang terhubung melalui internet (*Internet of Things*)(Muktiawan & Nurfiiana, 2018). Masyarakat juga sudah mulai banyak menghabiskan waktu untuk berselancar diinternet dengan berbagai keperluan melalui perangkat yang dimilikinya. Hal tersebut bahkan sudah menjadi budaya baru bagi kebanyakan masyarakat di Indonesia. Dengan dukungan teknologi dan sistem canggih tersebut banyak aktifitas maupun pekerjaan masyarakat menjadi terbantu, tetapi dibalik semua itu tentu saja juga ada bahaya yang sering tidak disadari oleh penggunanya, misalkan seperti masalah keamanan atau kerahasiaan data pengguna.

Permasalahan terkait *security* dan privasi data menjadi persoalan yang cukup penting karena hingga sekarang tidak sedikit pengguna yang pernah menjadi korban pencurian, pengrusakan, maupun modifikasi file atau data digitalnya. Bagi para pelaku kegiatan tersebut, file digital para korban bisa dimanfaatkan dalam mencari keuntungan untuk mereka ataupun pihak lain yang memerlukan untuk berbagai hal dan tentu saja akan menjadi suatu kerugian besar bagi korban.

Kasus kejahatan digital yang sering terjadi adalah jenis pencurian, pengrusakan, maupun modifikasi file gambar digital yang dalam hal ini adalah foto atau gambar bersifat *private* yang disimpan pada *cloud storage* maupun *local storage* perangkat pengguna. File foto *private* pengguna tersebut menjadi tersebar luas dan menjadi konsumsi publik dunia maya yang bisa mengakibatkan kerugian materil maupun moril dari pemilik foto digital tersebut.

Agar dapat meminimalisir masalah *security* dan privasi data digital dapat menggunakan metode kriptografi (*Cryptography*) yang

merupakan salah satu metode dalam pengamanan data. Kriptografi memiliki peranan yang sangat penting terhadap pengamanan alur pengiriman data-data melalui jaringan internet agar pihak yang tidak berkepentingan sulit untuk mengambil ataupun melihat data tersebut (Fadlan et al., 2021). Melalui metode tersebut, data asli dari file digital dikonversi kedalam bentuk data tersandi yang dikenal dengan enkripsi, dan sebaliknya mengkonversi data tersandi kebentuk data aslinya yang dikenal dengan dekripsi (Minarni, 2019). Dengan metode ini, file atau data digital disamarkan menjadi bentuk tersandi tanpa makna, sehingga bagi yang bukan pemilik file atau data tersebut akan sulit mengetahui bentuk file atau data aslinya. Secara umum teknik pengkodean data dengan metode kriptografi terbagi menjadi dua berdasarkan penggunaan jenis sandinya, yaitu metode simetris dan metode asimetris (Malvi & Painem, 2020).

Penelitian yang sebelumnya dilakukan oleh Tio Lovian dan Iskandar Fitri (2022) berjudul "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang" melakukan enkripsi data input barang dengan algoritma Base64 (Lovian & Fitri, 2022). Pengamanan data juga dilakukan oleh Widiarti Rista Maya, dkk. (2022) dengan algoritma DES melalui penelitian yang berjudul "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES" (Rista Maya et al., 2022). Selain pengamanan data input dari database sistem, teknik kriptografi juga bisa dilakukan untuk pengamanan file teks seperti pada penelitian yang berjudul "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5" dilakukan oleh Ahmad Zaki Fadilla Rangkuti dan Hasanul Fahmi (2020) (Zaki Fadilla Rangkuti et al., 2020). Penelitian terdahulu yang berjudul "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android" oleh Angga Aditya Permana (2018) melakukan pengamanan pesan teks dengan metode Vigenere Cipher untuk pengguna android (Aditya Permana, 2018). Sedangkan pengamanan pesan teks yang dilakukan oleh Sugeng Murdowo (2019) menggunakan algoritma Electronic Code Book (ECB) pada penelitian yang berjudul "Mengenal Kriptografi Modern Sederhana Menggunakan Elektronik Code Book (ECB)" (Murdowo, 2019).

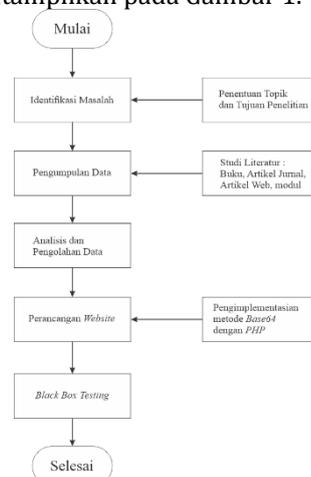
Berdasarkan permasalahan diatas, maka peneliti mencoba untuk mengimplementasikan metode kriptografi tersebut kedalam sebuah sistem dengan algoritma Base64 untuk menerjemahkan data biner berbentuk ASCII (American Standard Code for Information Interchange) yang merupakan suatu standar

pengkodean karakter huruf, angka maupun simbol ini bisa ditemukan pada keyboard perangkat komputer maupun *smartphone* dan perangkat digital lainnya. Pada ASCII terdapat lima (5) karakter kontrol yang dikelompokkan berdasarkan penggunaannya seperti *logical communication*, *Device control*, *Information separator*, *Code extention*, serta *physical communication* (Tantoni & Taufan Asri Zaen, 2018). Sehingga file gambar atau foto digital yang ingin dilindungi akan di enkripsi (*encryption*) kedalam bentuk teks (*ciphertext*) dan juga dapat mengembalikannya ke bentuk file aslinya dengan proses deskripsi (*decryption*).

## II. BAHAN DAN METODE

### Tahapan Penelitian

Tahapan yang dilakukan pada penelitian ini dimulai dengan melakukan identifikasi masalah yang melingkupi penentuan topik dan tujuan penelitian. Kemudian melakukan pengumpulan data-data terkait topik penelitian melalui studi literatur. Data-data penelitian yang sudah terkumpul dianalisis dan diolah sesuai kebutuhan dalam penelitian terutama yang berhubungan dengan metode Base64 dan perancangan website. Selanjutnya dilakukan pengimplementasian metode Base64 kedalam bahasa pemrograman PHP untuk dijadikan dalam bentuk sistem berbasis website yang dapat digunakan secara online. Tahap terakhir dilakukan Black Box Testing yang merupakan salah satu metode pengujian perangkat lunak. Melalui Black Box Testing pengujian sistem dapat dilakukan dengan mudah dan cepat karena pengujian tanpa memperhatikan detail sistem, hanya berfokus pada fungsionalitas sistemnya saja yang mana pada saat pengujian sistem tidak berfungsi sebagaimana mestinya akan dilakukan revisi perancangan kembali (Febriyanti et al., 2021). Tahapan penelitian tersebut ditampilkan pada Gambar 1.



Gambar 1. Flowchart Tahapan Penelitian

### Algoritma Base64

Algoritma *Base64* adalah suatu algoritma yang dapat melakukan proses *Encoding* maupun proses *Decoding* bentuk plainteks atau data menjadi karakter *ASCII*, berdasarkan bilangan dasar 64 atau merupakan cara untuk melakukan proses penyandian data biner. Pada proses transformasi *Base64*, sejumlah karakter yang dapat dihasilkan adalah dari huruf A sampai Z, a sampai z, angka 0 sampai 9, simbol +, /, dan = (karakter "=" ini dipakai sebagai penyesuaian serta untuk menggenapkan jumlah data biner, karakter "=" dikenal juga sebagai pengisi pad) (Ginting & Ginting, 2017). Pada dunia maya atau Internet, transformasi *Base64* sering dipakai sebagai media dalam pengiriman data, hal ini dikarenakan data yang dihasilkan melalui proses encode *Base64* adalah plainteks, oleh karena itu data tersebut menjadi lebih mudah untuk dikirim, tidak seperti data yang dikirimkan dalam bentuk biner. Sebenarnya algoritma *Base64* bukanlah enkripsi, tetapi suatu standar dalam melakukan proses penyandian pesan/data (*Encoding*) (Supiyandi et al., 2020).

Tabel 1. Kode Index Base64

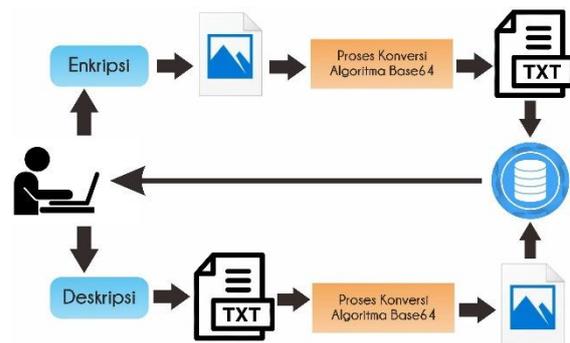
Value	Char	Value	Char	Value	Char
0	A	22	W	44	s
1	B	23	X	45	t
2	C	24	Y	46	u
3	D	25	Z	47	v
4	E	26	a	48	w
5	F	27	b	49	x
6	G	28	c	50	y
7	H	29	d	51	z
8	I	30	e	52	0
9	J	31	f	53	1
10	K	32	g	54	2
11	L	33	h	55	3
12	M	34	i	56	4
13	N	35	j	57	5
14	O	36	k	58	6
15	P	37	l	59	7
16	Q	38	m	60	8
17	R	39	n	61	9
18	S	40	o	62	+
19	T	41	p	63	/
20	U	42	q		(pad) =
21	V	43	r		

### III. HASIL DAN PEMBAHASAN

#### Proses Enkripsi dan Deskripsi Algoritma Base64 Pada Sistem

Proses enkripsi dan deskripsi dari algoritma *Base64* akan diimplementasikan kedalam suatu aplikasi berbasis web yang dirancang menggunakan bahasa pemrograman PHP. Didalam pemrograman PHP telah tersedia suatu fitur yang dapat dimanfaatkan untuk membantu proses enkripsi serta deskripsi menggunakan metode *Base64*, yaitu dengan perintah :

- a. *Base64\_encode()* : perintah untuk meng-encode atau enkripsi.
- b. *Base64\_decode()* : perintah untuk meng-decode atau deskripsi.



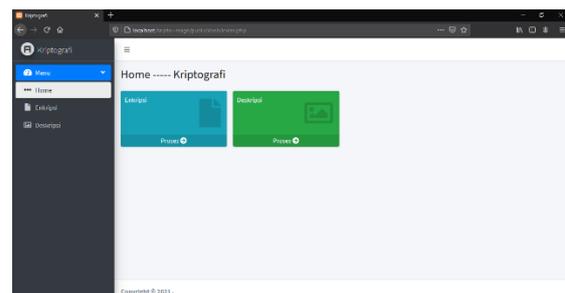
Gambar 2. Arsitektur sistem

### Implementasi

Proses kriptografi gambar digital pada penelitian ini dilakukan dengan algoritma *Base64* yang diimplementasikan kedalam aplikasi berbasis web yang dirancang menggunakan bahasa pemrograman PHP. Adapun tahapan penggunaan serta hasil pengujian yang didapatkan sebagai berikut:

- a. Penggunaan Sistem
  1. Halaman Utama

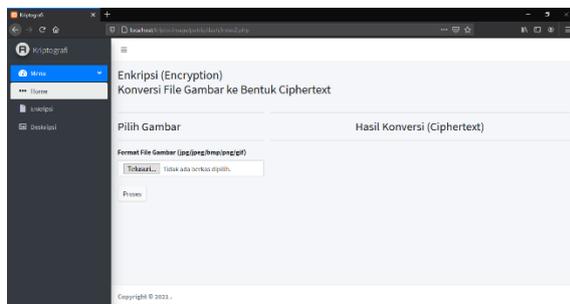
Halaman ini merupakan halaman yang pertama kali tampil saat sistem diakses. Pada halaman ini terdapat dua (2) pilihan menu yaitu enkripsi dan deskripsi. Jika memilih (klik) menu enkripsi, maka sistem akan berpindah kehalaman proses enkripsi. Dan jika yang dipilih (klik) menu deskripsi, maka sistem akan berpindah kehalaman proses deskripsi.



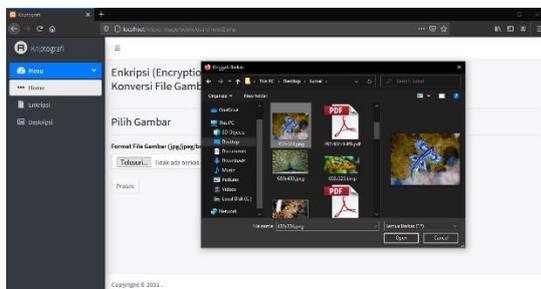
Gambar 3. Halaman utama

## 2. Proses Enkripsi

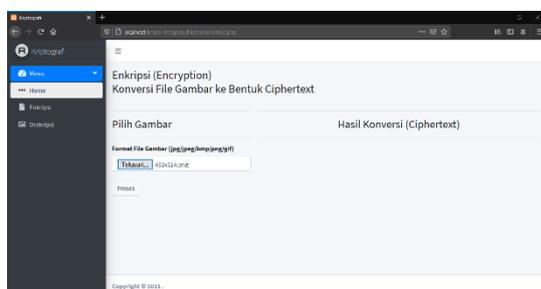
Pada halaman ini pengguna dapat melakukan proses enkripsi pada gambar digital menjadi bentuk *ciphertext* (file txt). Untuk mengubah gambar digital menjadi bentuk teks terenkripsi, pengguna dapat menekan (klik) tombol telusuri dan mencari lokasi dari gambar digital yang akan di enkripsi. Setelah gambar dipilih, kemudian tekan tombol proses dan hasil teks (*ciphertext*) yang telah terenkripsi melalui proses algoritma *Base64* akan muncul pada kolom teks disampingnya. Jika pengguna ingin menyimpan hasil teks terenkripsi tersebut kedalam bentuk file txt, dapat dilakukan dengan menekan (klik) tombol *download text* dan simpan kelokasi yang diinginkan.



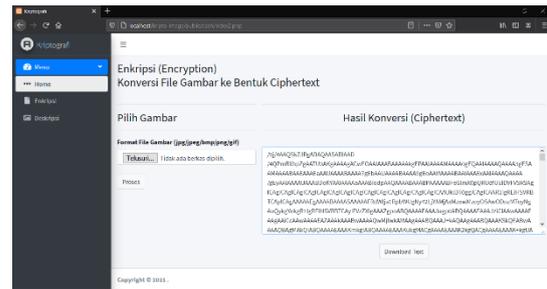
Gambar 4. Halaman proses enkripsi



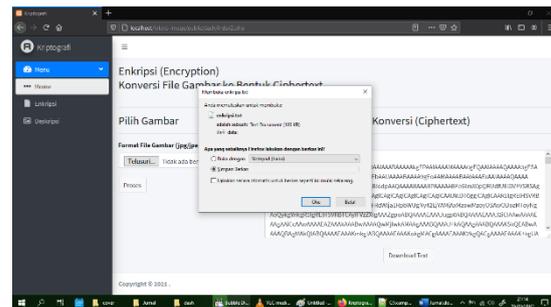
Gambar 5. Pemilihan file gambar



Gambar 6. Pemrosesan enkripsi



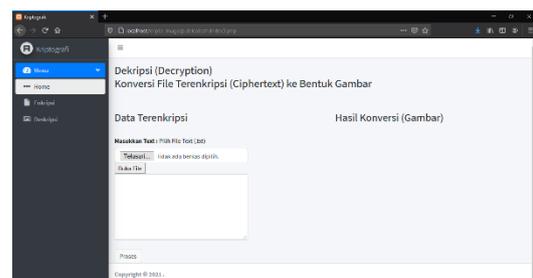
Gambar 7. Hasil enkripsi gambar



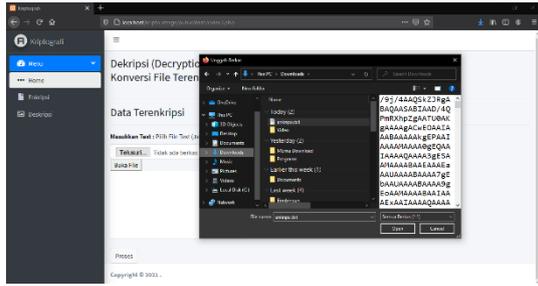
Gambar 8. Penyimpanan hasil teks terenkripsi

## 3. Proses Deskripsi

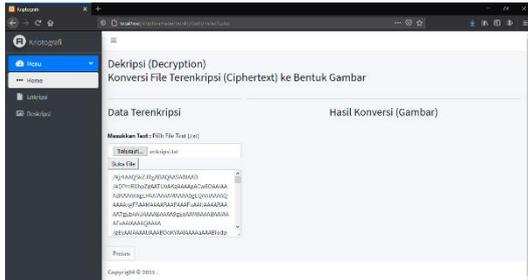
Pada halaman ini pengguna dapat melakukan proses deskripsi dari *ciphertext* yang berupa file text (txt) terenkripsi menjadi bentuk file aslinya, yaitu file gambar digital. Untuk mengubah *ciphertext* menjadi file gambar digital, pengguna dapat menekan (klik) tombol telusuri dan mencari lokasi dari file *ciphertext* (txt) yang akan dilakukan proses deskripsi. Setelah file *ciphertext* dipilih, kemudian tekan tombol buka file dan isi dari file *ciphertext* tersebut akan muncul pada kolom text dibawahnya. Selanjutnya tekan (klik) tombol proses dan hasil dari file *ciphertext* akan di deskripsi melalui proses algoritma *Base64* dikembalikan menjadi file gambar digital dan akan dimunculkan pada kolom disampingnya. Jika pengguna ingin menyimpan file gambar hasil deskripsi tersebut, dapat dilakukan dengan menekan (klik) kanan mouse dan pilih simpan gambar.



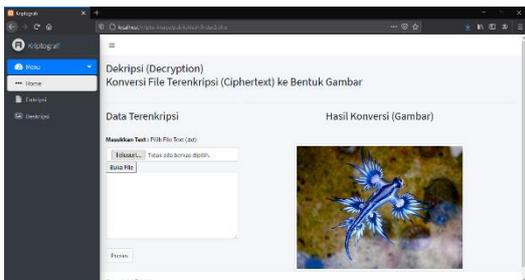
Gambar 9. Halaman proses deskripsi



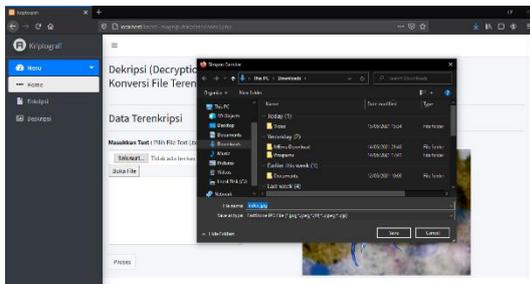
Gambar 10. Pemilihan file *ciphertext*



Gambar 11. Pemrosesan deskripsi



Gambar 12. Hasil deskripsi *ciphertext*



Gambar 13. Penyimpanan hasil deskripsi

b. Hasil Pengujian

Pada penelitian ini dilakukan proses enkripsi dan deskripsi masing-masing sebanyak 5 kali dengan file gambar digital yang berbeda. Berikut hasil pengujian yang telah dilakukan:

Tabel 2. Hasil Pengujian Enkripsi Algoritma *Base64* dengan PHP

No	Gambar	Ukuran <i>Pixel</i>	Format File	Ukuran File	Ukuran File Setelah Enkripsi (.txt)
----	--------	---------------------	-------------	-------------	-------------------------------------

1		432 x 324	PNG	75,0 KB	100KB
2		600 x 400	JPEG	137KB	183KB
3		650 x 325	BMP	283KB	378KB
4		1200 x 675	JPG	212KB	283KB
5		2500 x 1674	JPG	565KB	755KB

Berdasarkan hasil pengujian pada Tabel 2, semua file gambar digital dengan format berbeda (PNG, BMP, JPEG, JPG) dan ukuran *Pixel* yang berbeda berhasil dikonversi menjadi file terenkripsi (*ciphertext*), hanya saja ukuran file hasil enkripsi yang disimpan dalam format txt menjadi lebih besar dibandingkan ukuran file aslinya (format gambar).

Tabel 3. Hasil Pengujian Deskripsi Algoritma *Base64* dengan PHP

No	Ukuran <i>Pixel</i>	Format File	Ukuran File	Hasil Setelah Proses Deskripsi
1	432x324	PNG	75,0KB	
2	600x400	JPEG	137KB	
3	650x325	BMP	283KB	
4	1200x675	JPG	212KB	
5	2500x1674	JPG	565KB	

Berdasarkan hasil pengujian pada Tabel 3, semua file *ciphertext* (txt) dari hasil proses enkripsi sebelumnya dapat dikembalikan ke file aslinya (gambar digital) tanpa kehilangan kualitas atau ketajaman warnanya, ukuran *Pixel* serta ukuran filenya juga kembali seperti semula.

IV. KESIMPULAN

Berdasarkan hasil implementasi metode kriptografi yang telah dilakukan pada penelitian ini, dapat disimpulkan bahwa algoritma *Base64* yang digunakan pada bahasa pemrograman PHP dapat melakukan proses enkripsi dan deskripsi file gambar digital dengan baik. Walaupun pada saat dilakukan proses enkripsi, hasil yang didapat dari ukuran file *ciphertext* yang berformat txt menjadi lebih besar daripada ukuran file gambar digitalnya. Tetapi saat dilakukan proses deskripsi dengan mengubah file *ciphertext* menjadi file gambar digital, ukuran filenya kembali ke ukuran semula sesuai file gambar aslinya yang sebelum dilakukan proses enkripsi. Algoritma

Base64 dapat dijadikan alternatif bagi peneliti atau perancang sistem dengan pemrograman PHP lainnya dalam membuat perangkat lunak untuk enkripsi (*encode*) dan deskripsi (*decode*) teks maupun file karena pada PHP sudah menyediakan fungsi tersebut, sehingga cukup memudahkan dalam implementasinya. Selain itu dengan berhasilnya implementasi metode kriptografi ini akan dapat membantu pengguna dalam mengamankan file gambar digital yang dianggap penting atau *private* menjadi bentuk file teks yang terenkripsi, sehingga tidak bisa dilihat oleh orang yang tidak berhak atau tidak memiliki izin.

## V. REFERENSI

- Aditya Permana, A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, 4(3).
- Fadlan, M., Rosmini, R., & Haryansyah, H. (2021). Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 5(3), 806. <https://doi.org/10.30865/mib.v5i3.3019>
- Febriyanti, N. M. D., Sudana, A. A. K. O., & Piarsa, I. N. (2021). Implementasi Black Box Testing pada Sistem Informasi Manajemen Dosen. *JITTER- Jurnal Ilmiah Teknologi Dan Komputer*, 2(3).
- Ginting, N. F., & Ginting, M. (2017). Perbandingan Kriptografi RSA dengan Base64. *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)*, 2(2), 2548-1916.
- Lovian, T., & Fitri, I. (2022). Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 6(1), 692. <https://doi.org/10.30865/mib.v6i1.3513>
- Malvi, A., & Painem. (2020). Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF). *JURNAL INFORMATIK*, 16(2).
- Minarni, R. (2019). Implementasi Algoritma Base64 untuk Mengamankan SMS pada Smartphone. *Technology and Science (BITS)*, 1(1), 28-33.
- Muktiawan, D. A., & Nurfiana. (2018). SISTEM MONITORING PENYIMPANAN KEBUTUHAN POKOK BERBASIS INTERNET OF THINGS (IoT). *Jurnal Manajemen Sistem Informasi Dan Telematika*, 9(1).
- Murdowo, S. (2019). MENGENAL KRIPTOGRAFI MODERN SEDERHANA MENGGUNAKAN ELECTRONIK CODE BOOK (ECB). *INFOKAM*, 15(1).
- Rista Maya, W., Komputer, T., Triguna Dharma, S., & Komputer, S. (2022). Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES. *Jurnal Sains Manajemen Informatika Dan Komputer*, 21(1), 1-9. <https://ojs.trigunadharma.ac.id/index.php/jis>
- Supiyandi, S., Hermansyah, H., & Sembiring, K. A. P. (2020). Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 4(2), 340. <https://doi.org/10.30865/mib.v4i2.2042>
- Tantoni, A., & Taufan Asri Zaen, M. (2018). IMPLEMENTASI DOUBLE CAESAR CIPHER MENGGUNAKAN ASCII. *Jurnal Informatika & Rekayasa Elektronika*, 1(2). <http://e-journal.stmiklombok.ac.id/index.php/jire>
- Wijayanti, Yunarti, S., & Harmaningsih, D. (2022). Proyeksi Masyarakat 5.0 Melalui Model Pembelajaran Berlandaskan HOTS Di Perguruan Tinggi. *Jurnal IKRAITH-HUMANIORA*, 6(1).
- Zaki Fadilla Rangkuti, A., Fahmi, H., & Pelita Nusantara, S. (2020). Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5. *Jurnal Nasional Komputasi Dan Teknologi Informasi*, 3(2).