APPLICATION OF FILE TO IMAGE ENCRYPTION (FTIE) USING RANDOMIZED TEXT AND ARNOLD CAT MAP (ACM) ALGORITHM BASED ON WEBSITE FOR DIGITAL DATA SECURITY

Johdhy Prasojo[1], Yudi Prayudi[2]
Teknik Informatika
Universitas Islam Indonesia (UII)
Yogyakarta, Indonesia
[1]Johdhy.prasojo@gmail.com, [2]prayudi@uii.ac.id

***Abstract*—Data security and information are needed to maintain and protect the confidentiality of data. One of the data security techniques is to use encryption and decryption techniques. The encryption and decryption techniques that will be used in this study are the File To image Ecnryption (FTIE) technique using the Randomized Text algorithm and the Arnold Cat Map (ACM) algorithm. FTIE is a technique developed from the Text To Image Encryption (TTIE) technique. Randomized Text is an algorithm that is dynamic chiper. The reason for using Randomized Text is because each Randomized Text algorithm encryption will produce different data even though it has used the same key. Randomized Text has a random value that will produce a different data, because the results of different values will increase the security of a data when encrypted. The Arnold Cat Map (ACM) algorithm is an algorithm that will be used in this research as a randomization of the pixel position of an image, the Arnold Cat Map (ACM) encryption technique used in encrypting an image. In this study the ACM algorithm will randomize the position of an image, the result will get a good enough security when combined with the Randomized Text algorithm. Using PHP, Html, Javascript and all the design and implementation will produce an FTIE website application.**

Keywords—FTIE, TTIE, Arnold Cat Map (ACM), Randomized Text, PHP, Html, Javascript.

I. PENDAHULUAN

Seiring dengan kemajuan teknologi komputer dan dunia digital yang berkembang pesat telah menjadi kebutuhan primer untuk munculnya inovasi pada aplikasi berbasis website di era yang modern saat ini. Inovasi yang terus bermunculan tersebut akan berdampak negatif pada sistem keamanan dalam pertukaran informasi yang menyebabkan penyadapan data.

Salah satu teknik pengamanan data adalah menggunakan teknik enkripsi dan dekripsi. Enkripsi dan dekripsi merupakan bidang ilmu kriptografi. (Nurdin Nurdin & Prayitno, 2017) menjelaskan bahwa algoritma kriptografi merupakan suatu bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi dengan mengkonversi data ke bentuk kode-kode tertentu sehingga informasi tidak dapat terbaca oleh pihak yang tidak berkepentingan.

Selain itu, untuk menghasilkan informasi yang lebih aman dalam pembuatan aplikasi ini akan digunakan penggabungan algoritma antara algoritma *Randomized Text* dengan *Arnold Cat Map* (ACM). Tujuan memilih algoritma *Randomized Text* karena algoritma ini merupakan salah satu dari jenis *randomized encryption*. (Maurer, 1992) menyatakan bahwa *chipertext* dapat disempurnakan jika memliki kunci rahasia yang sama besar dengan *plaintextnya*. Akan tetapi penggunaan algoritma *Randomized encryption* masih memiliki celah keamanan yaitu *chipertext* yang dihasilkan masih memiliki pola, oleh karena itu dibutuhkan salah satu algoritma transformasi untuk menghilangkan pola tersebut. Tujuan memilih algoritma *Arnold Cat Map* (ACM) dikarenakan algoritma ACM menurut (Ronsen, Halim, & Syahputra, 2014) memiliki tingkat keamanan yang rendah dan transformasi yang sederhana, tetapi sangat untuk mengacak posisi *chipertext* dari *randomized text*.

Oleh karena itu, dibutuhkan sebuah aplikasi keamanan informasi yang tidak dapat dibaca oleh kriptanalisis. Salah satunya adalah dengan teknik enkripsi *File To Image Encryption* (FTIE) menggunakan algoritma *Randomized Text* dan algoritma *Arnold Cat Map* (ACM). Dari uraian diatas maka akan dibuat sebuah aplikasi *File To Image Encryption* (FTIE) dengan menggunakan algoritma *Randomized Text* dan *Arnold Cat Map* (ACM) berbasis website untuk keamanan data digital yang nantinya aplikasi berbasis web tersebut akan digunakan sebagai pengamanan sebuah informasi data.

II. STUDI PUSTAKA

A. Randomized Text

Randomized text adalah salah satu teknik enkripsi yang algoritmanya bersifat dinamis artinya algoritma ini selalu menghasilkan pengacakan walaupun dari *plaintext* yang sama dengan kunci yang sama pula. *Randomized text* adalah algoritma kriptografi yang di temukan oleh (Munir, 2012).

Pada gambar di atas adalah flowchat dari teknik enkripsi *randomized text*. *Flowchart* tersebut terdiri dari input *file*,

applying encryption technique, random *function*, use *appropriate key index*, *end of file*, dan *output file*. *Randomized* memliki persamaan enkripsi yang sederhana yaitu:

C1 = K + 2P + R

C2 = 2K + P + R

Randomized Text melakukan enkripsi per-karakter dengan persamaan diatas, setiap satu karakter dari *plaintext* akan menghasilkan 2 karakter . Sehingga tiap kali melakukan enkripsi, yang dihasilkan pasti akan menghasilkan dua kali lipat dari ukuran *plaintext*. Sedangkan persamaan dekripsinya adalah :

P = (C1-K) – (C2-2K)

Pada saat proses dekripsi ukuran plaintext akan menjadi setengah dari ukuran.

B. *Anold Cat Map (ACM)*

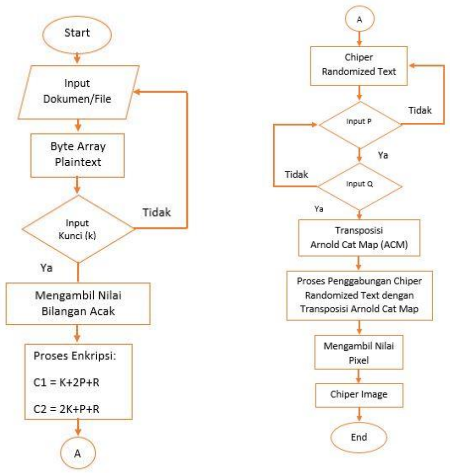
Menurut (Munir, 2012) *Arnold Cat Map* (ACM) merupakan fungsi *chaos* dwimatra dan bersifat *reversible*. Fungsi chaos ini ditemukan oleh Vladimir Arnold pada tahun 1960, dan kata "*cat*" muncul karena dia menggunakan citra seekor kucing dalam eksperimennya. ACM mentransformasikan koordinat (x, y) di dalam citra yang berukuran N x N ke koordinat baru (x', y'). Persamaan iterasinya adalah

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \quad (1)$$

yang dalam hal ini (xi, yi) adalah posisi pixel di dalam citra, (xi+1, yi+1) posisi *pixel* yang baru setelah iterasi ke-i; b dan c adalah integer positif sembarang. Determinan matriks harus sama dengan 1 agar hasil trans*form*asinya bersifat *area-preserving*, yaitu tetap berada di dalam area citra yang sama. ACM termasuk pemetaan yang bersifat satu-ke-satu karena setiap posisi *pixel* selalu ditransformasikan ke posisi lain secara unik. ACM diiterasikan sebanyak m kali dan setiap iterasi menghasilkan citra yang acak. Nilai b, c, dan jumlah iterasi m dapat dianggap sebagai kunci rahasia.

III. METODOLOGI

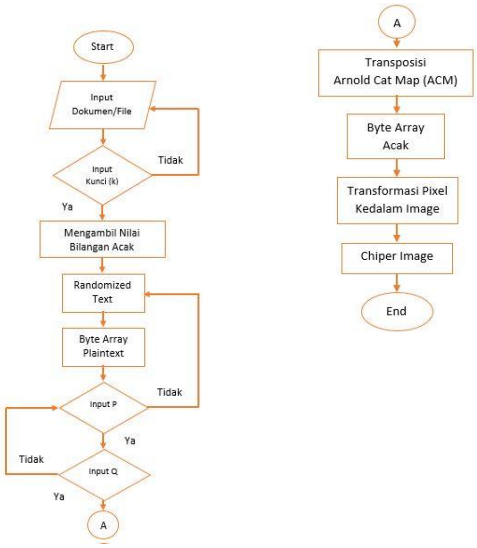
Pada rancangan ini akan dibuat penggabungan algoritma *Randomized Text* dan *Arnold Cat Map* yang nantinya akan terbentuk *flowchart* skema dari *File To Image Encryption* (FTIE). Gambar 3.1 adalah perancangan dari *flowchart* skema FTIE dengan menggunakan algoritma *Randomized Text* dan *Arnold Cat Map*.



Gambar 2. *Flowchart* tahapan FTIE dengan menggunakan algoritma *Randomized Text* dan *Arnold Cat Map*

A. *Perancangan Model Enkripsi*

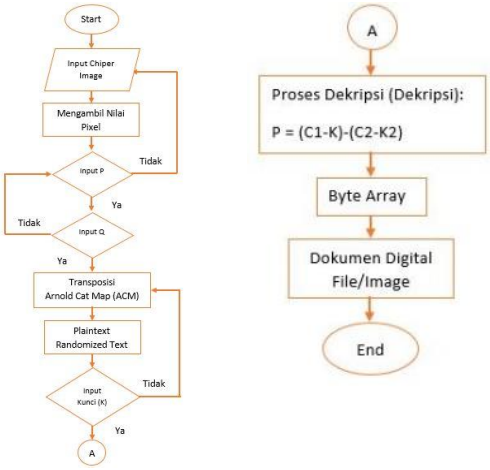
Enkripsi merupakan proses untuk mengamankan suatu informasi agar informasi tersebut tidak dapat diketahui oleh orang lain. Pada tahapan ini akan dibuat *flowchart* perancangan model enkripsi dari sebuah *file* dan hasil akhirnya akan terbentuk sebuah gambar.



Gambar 3. *Flowchart* Perancangan Model Enkripsi FTIE

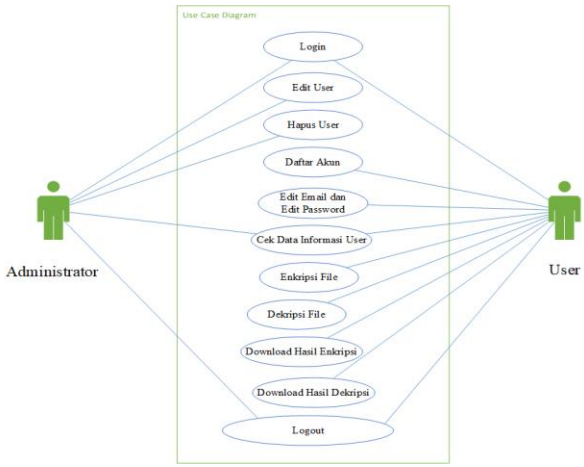
B. *Perancangan Model Dekripsi*

Pada tahapan ini akan di buat *flowchart* perancangan model dekripsi dimulai dari proses mengambil file dan mengambil nilai pixel serta tahapan-tahapan transposisi ACM dari sebuah gambar dan hasil akhirnya berupa dokumen digital/*file*.



Gambar 4. *Flowchart* Perancangan Model Enkripsi FTIE

C. Use Case Diagram

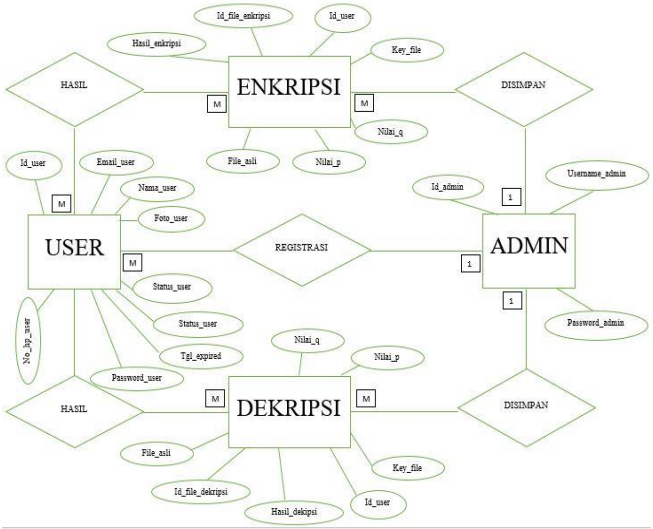


Gambar 5. *Use* Case Diagram

Pada *Use Case* Diagram di atas, maka dapat mendiskripsikan hal-hal sebagai berikut:

- Administrator dan *user* merupakan *Actor*.
- Administrator dan *user* dapat melakukan *login*, cek data informasi *user* dan *logout*.
- Administrator fungsionalitas adalah: *login*, *edit user*, hapus *user*, cek data informasi *user* dan *logout*.
- *User* fungsionalitas adalah: *login*, daftar, cek data informasi *user*, enkripsi, dekripsi, *download* hasil enkripsi, *download* hasil dekripsi, *logout*.

D. Entity Realationship Diagram

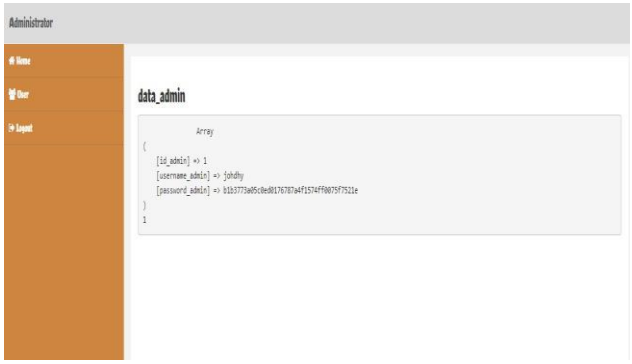


Gambar 6. ERD

IV. HASIL DAN PEMBAHASAN

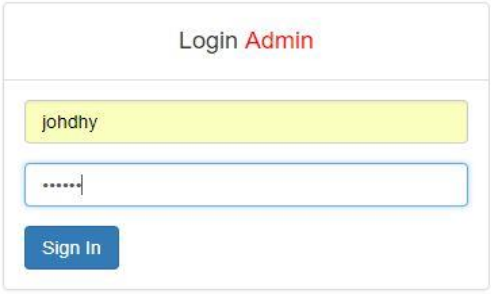
A. Antar Muka Admin

Pada halaman *home* admin ini terdapat tiga tampilan menu dan tampilan data admin. Tampilan menu tersebut meliputi, menu *home*, menu *user* dan menu *logout*.



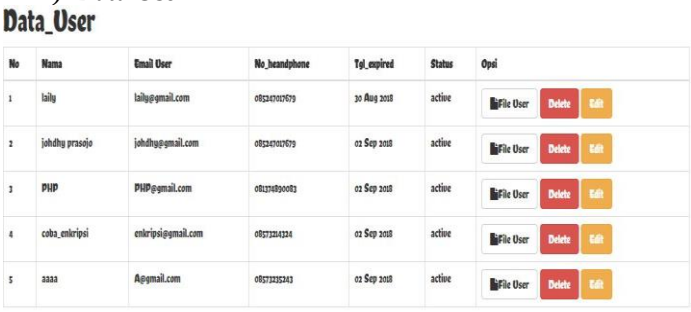
Gambar 7. *Home* admin

1) Login admin



Gambar 8. *Login* admin

2) Data User



Gambar 9. Data *User*

3) Edie User

Gambar 10. *Edit user*

4) File User

a) File asli

Gambar 11. *File* asli

\

b) File enkripsi

Gambar 12. *File* enkripsi

5) Logout

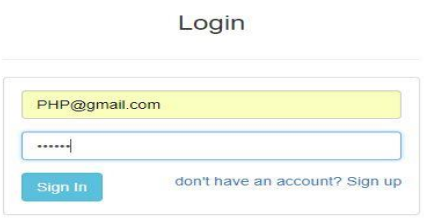
Gambar 13. *Logout*

B. Antar Muka User

Gambar 15. *Home user*

Pada halaman *home user* ini terdapat lima tampilan menu dan tampilan cara pemakaian aplikasi enkripsi dan dekripsi. Tampilan menu tersebut meliputi, menu *home*, menu *profile*, menu *encryption*, menu *decryption* dan menu *logout*.

1) Login user

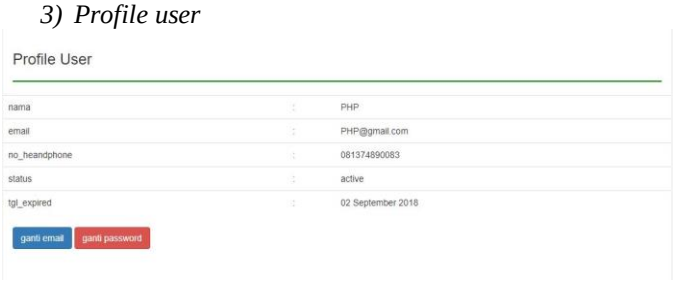


Gambar 14. *Login user*

2) Daftar user

Gambar 15. Daftar *user*

3) Profile user



Gambar 16. *Profile user*

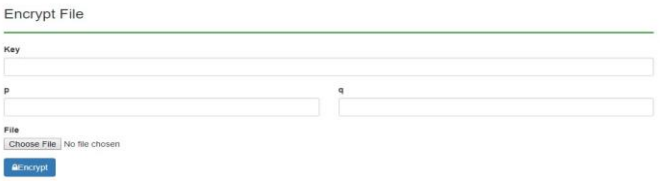
a) Edit email user

Gambar 17. *Edit email user*

b) Edit password user

Gambar 18. *Edit password user*

C. Antarmuka Enkripsi



Gambar 19. Halaman enkripsi

a) Pengujian aplikasi enkripsi

Adapun dokumen digital yang akan digunakan untuk bahan pengujian dapat dilihat pada Tabel 4.1 dibawah ini:

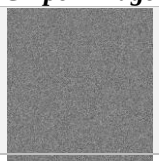
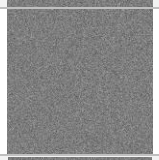
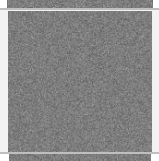
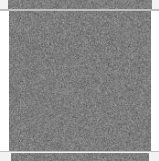
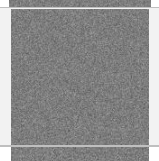
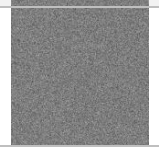
Tabel 1. Bahan pengujian

Nama *File*	**Ukuran (*bytes*)**	**Tipe *File***
Percobaan docx	2.314.240	*World document*
Percobaan pdf	2.276.352	Pdf *document*
Percobaan	4.641.792	MP4 *File*

mp4		
Percobaan mp3	3.365.888	MP3 *format sounds*
Percobaan jpg	1.613.824	Jpg *File*
Percobaan pptx	334.848	Pptx *document*

Pada tabel dibawah ini merupakan hasil enkripsi dari tabel 4.1 untuk hasilnya sebagai berikut:

Tabel 2. Hasil pengujian

Nama *File*	**Kunci**	***Chiper Image***
Percobaan docx	k = 100 p = 353 q = 123	
Percobaan pdf	k = 40 p = 602 q = 432	
Percobaan mp4	k = 30 p = 121 q = 44	
Percobaan rar	k = 333 p = 222 q = 111	
Percobaan jpg	k = 100 p = 100 q = 100	
Percobaan pptx	k = 321 p = 876 q = 123	

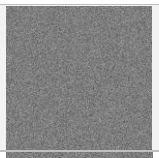
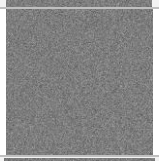
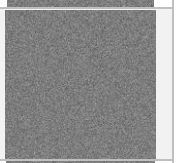
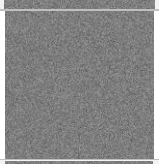
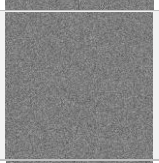
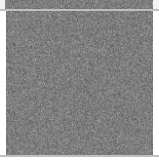
D. Antarmuka Dekripsi

Gambar 20. Halaman dekripsi

a) Pengujian hasil dekripsi

Adapun *file chiper image* yang akan digunakan untuk bahan pengujian dapat dilihat pada Tabel 4.3 dibawah ini:

Tabel 3. bahan pengujian (*chiper image*)

Nama *File*	**Kunci**	***Chiper Image***
20180804020843_percobaan_docx	k = 100 p = 353 q = 123	
20180804021045_percobaan_pdf	k = 40 p = 602 q = 432	
20180804021211_percobaan_mp4	k = 30 p = 121 q = 44	
20180804021930_percobaan_rar	k = 333 p = 222 q = 111	
20180804021558_percobaan_jpg	k = 100 p = 100 q = 100	
20180804021502_percobaan_pptx	k = 321 p = 876 q = 123	

Pada tabel dibawah ini merupakan hasil dekripsi dari tabel 4.3 untuk hasilnya sebagai berikut:

Tabel 4. Hasil Dekripsi

Nama *File*	**File dekripsi**
20180804023729_percobaan	
20180804023905_percobaan	
20180804024503_percobaan	
20180804024740_percobaan	
20180804024822_percobaan	

20180804025001_percobaan	Hasil Dekripsi dari chiper image 20180804021502_percobaan_pptx.png 

E. Perbadaan penelitian

Tabel 5. Perbedaan penelitian

Aplikasi *File To Image Encryption* (FTIE) menggunakan algoritma *Randomized Tex*t dan *Arnold Cat Map* (ACM) berbasis Website untuk keamanan data digital.	Aplikasi *File To Image Encryption* (FTIE) menggunakan algoritma *Randomized Tex*t dan *Arnold Cat Map* (ACM) untuk keamanan data digital.
Aplikasi ini berbasis website dengan menggunakan bahasa pemrograman PHP, *Html* dan *Javascript*.	Aplikasi ini berbasis desktop dengan menggunakan bahasa pemrograman C#.
Output yang dihasilakan merupakan suatu aplikasi website yang tujuannya dapat digunakan secara online.	*Output* aplikasi ini hanya bisa di gunakan pada persatuan komputer digital saja dan tidak bisa di onlinekan.
Lebih banyak mengulas implementasi program.	Lebih banyak melakukan analisis program.
Chiper image yang dihasilkan berupa pixel R, G, B hitam dan putih.	*Chiper image* yang dihasilkan berupa pixel R, G, B berwarna.
Tidak hanya melakukan proses enkripsi dan dekripsi, lebih banyak fitur didalam aplikasi website ini. Contohnya seperti penggunaan hak akses admin dan hak akses *user*.	Hanya dapat melakukan enkripsi dan dekripsi.
Semua proses enkripsi dan dekripsi tersimpan di *database*.	Semua proses enkripsi dan dekripsi langsung dari aplikasi.

V. KESIMPULAN

Berdasarkan hasil yang didapat dalam pembuatan tugas akhir aplikasi berbasis website ini, maka dapat diambil kesimpulan sebagai berikut:

1. Teknik FTIE terbagi menjadi 2 tahap, yiatu tahap enkripsi menggunakan algoritma *Randomized Text* dan *Arnold Cat Map* dan dekripsi menggunakan algoritma *Randomized text* dan *Arnold Cat Map*.
2. Aplikasi web FTIE yang dibangun menggunakan pemrograman PHP, *Html* dan *Javascript*. Implementasi aplikasi web ini mengunakan XAMPP *localhost*. Sedangkan untuk penyimpanan data *user* dan admin menggunakan *database* Mysql.
3. Aplikasi web FTIE yang dibangun terbagi menjadi 2 tampilan web, yaitu tampilan administrator dan tampilan *user*.
4. Aplikasi web FTIE yang dibangun akan menghasilkan gambar *chiper image* dari proses enkripsi dan *file* asli dari proses dekripsi, data enkripsi dan dekripsi akan disimpan kedalam *database* Mysql.
5. Proses enkripsi dan dekripsi berjalan baik, proses enkripsi menggunakan teknik FTIE memiliki ketahanan dan keamanan yang kuat terhadap kriptanalisis dan proses dekripsi menggunakan teknik FTIE memiliki integritas yang dapat dipertanggungjawabkan.

DAFTAR PUSTAKA

[1] Abidin, A. M., Hardianti, F., & Setiani, I. N. (2016). Analisa Dan Implementasi Proses Kriptografi *Encryption-Decryption* Dengan Algoritma Advanced *Encryption* Standard (Aes-128). *Jurnal Sarjana Teknik Informatika, Keamanan Komputer*, `1-20.

[2] Chrystanti, Y. C., & Wardati, I. U. (2011). Sistem Pengolahan Data Simpan Pinjam khusus Perempuan (SPP) Pada Unit Pengelola Kegiatan (UPK) Mitra Usaha Mandiri Program Nasional Pemberdayan Masyarakat Mandiri Perdesaan (PNPM-MPd) Kecamatan Pringkuku Kabupaten Pacitan. *Journal Speed – Sentra Penelitian Engineering Dan Edukasi*, *3*(1), 44–61. Retrieved from https://anzdoc.com/journal-speed-sentra-penelitian-engineering-dan-edukasi-volu8d7f8685b8b7fd6cbf53ac00eaa9d33c71098.html

[3] Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad. *Jurnal Nasional Informatika Dan Teknologi Jaringan*, *1*(1), 61–64.

[4] Hidayat, A. D., & Afrianto, I. (2017). Sistem Kriptografi Citra Digital pada Jaringan Intranet Menggunakan Metode Kombinasi Chaos Map dan Teknik Selektif. *Ultimatics*, *9*(1), 59–66.

[5] Kromodimoeljo, S. (2009). Teori & Aplikasi Kriptografi.

[6] Maurer, U. M. (1992). Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, *5*(1), 53–66. https://doi.org/10.1007/BF00191321.

[7] Munir, R. (2012). Robustness Analysis of Selective *Image Encryption* Algorithm Based on Arnold Cat Map Permutation. *Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics*, (December), 1–5.

[8] Nurdin Nurdin, & Prayitno, A. (2017). ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA MENGGUNAKAN ALGORITMA CIPHER TRANSPOSITION. *Jesik*, *3*(1), 1–11. Retrieved from nnurdin69@gmail.com.

[9] Ronsen, P., Halim, A., & Syahputra, I. (2014). Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm. *JSM STMIK Mikroskil*, *15*(2), 61–71.

[10] Santi, R. C. N. (2010). Implementasi Algoritma Enkripsi Playfair pada *File* Teks. *Teknologi Informatika DINAMIK*, *XV*(1), 27–33.

[11] Sari, D. I. (2016). Perancangan Aplikasi Kompresi Citra Dengan Metode Run Length Encoding Untuk Keamanan *File* Citra Menggunakan Caesar *Chiper*. *INFOTEK*, *1*(2), 43–47.

[12] Shanthi, & Palanisamy, D. V. (2014). A Novel Text to *Image Encryption* Technique by AES Rijndael Algorithm with Color Code Conversion. *IJETT*, *13*(5), 237–241.

[13] Suhartanto, M. (2012). Pembuatan Website Sekolah Menengah Pertama Negeri 3 Delanggu Dengan Menggunakan Php Dan Mysql. *Journal Speed – Sentra Penelitian Engineering Dan Edukasi*, *4*(1), 1–8. Retrieved from http://speed.web.id/ejournal/index.php/Speed/article/view/226.

[14] Suprianto, A., Prayudi, Y., & Sugiantoro, B. (2017). *File* To *Image Encryption* (FTIE) Menggunakan Algoritma Randomized Text Dan Arnold Cat Map (ACM) Untuk Keamanan Transmisi Data Digital. *HADFEX (Hacking and Digital Forensics Exposed)*, (August), 19–26.

[15] Yuliano, T. (2007). Pengenalan PHP. *Ilmiu Komputer*, 1–9.