KETIK : Jurnal Informatika
ISSN: 3026-183X (Media Online)
Vol. 01, No. 03, Januari 2024 Hal. 88-94
Faatuatua Media Karya
https://jurnal.faatuatua.com/index.php/KETIK

Implementasi Algoritma Freivalds pada Pembangkitan Kunci Algoritma Baufort Cipher

Taronisokhi Zebua

Universitas Budi Darma, Indonesia, email: taronizeb@gmail.com

Info Artikel

Diajukan: 08-02-2024
Diterima: 08-02-2024
Diterbitkan: 09-02-2024

Kata Kunci:
Kriptografi; Freivalds; Beaufort; Data; Teks

Keywords:
Criptography; Freivalds; Beaufort; Data; Text

Abstrak

Salah satu teknik yang dapat digunakan dalam mengamankan data penting dan bersifat rahasia adalah teknik kriptografi. Pengamanan data dengan teknik kriptografi bekerja berdasarkan algoritma pengamanan data, salah satunya adalah algoritma beaufort cipher. Konsep pengamanan data berdasarkan beuafort cipher adalah melakukan proses operasi elemen data yang diamankan dengan elemen kunci, sehingga masing-masing elemen data yang diamankan harus memiliki pasangan kunci. Konsep ini yang menyebabkan terjadinya perulangan penggunaan elemen kunci yang sama pada proses algoritma ini. Pemanfaatan elemen kunci yang berulang dalam teknik pebngamanan data sangat rentang dan tidak optimal pengamanannya, sehingga sangat mudah diserang oleh pihak lain. Salah satu solusi yang dapat digunakan adalah membangkitkan kata kunci secara otomatis untuk melengkapi elemen kata kunci yang kurang. Tentu proses ini dapat memanfaatkan algoritma yang adam salah satunya adalah algoritma freivalds. Algoritma ini lebih memprioritaskan pencocokan hasil operasi matriks baru berdasarkan nilai matriks input yang digunakan oleh pengguna, sehingga memungkinkan tidak terjadi perulangan kata kunci. Hal ini tentu dapat meningkatkan performa beuafort cipher dalam mengamankan data teks.

Abstract

One technique that can be used to secure important and confidential data is cryptographic techniques. Data security using cryptographic techniques works based on data security algorithms, one of which is the Beaufort Cipher algorithm. The concept of data security based on the feuafort cipher is to carry out operations on data elements that are secured with key elements, so that each data element that is secured must have a key pair. This concept causes the repeated use of the same key elements in this algorithm process. The use of repeated key elements in data security techniques is very broad and not optimal in security, so it is very easy to be attacked by other parties. One solution that can be used is to generate keywords automatically to complete the missing keyword elements. Of course, this process can utilize existing algorithms, one of which is the freivalds algorithm. This algorithm prioritizes matching the results of new matrix operations based on the input matrix values used by the user, thereby allowing keyword repetition to not occur. This can certainly improve the performance of the beuafort cipher in securing data text.

1. PENDAHULUAN

Pengamanan data penting merupakan salah satu hal penting yang harus dilakukan agar data yang bersifat rahasia dapat selalu terjaga orisinalitasnya. Salah satu teknik yang dapat digunakan untuk mewujudkan keamanan data penting atau rahasia adalah menggunakan teknik kriptografi. Teknik kriptografi mengamankan data dengan melakukan pengubahan terhadap data yang diamankan menjadi karakter-karakter lain yang berbeda dengan karakter data asli. Hal inilah yang dapat menyulitkan para penyerang untuk mendapatkan data asli. Berdasarkan penelitian terdahulu mengatakan bahwa teknik kriptografi yang dapat digunakan untuk memenuhi beberapa aspek penting dalam pengamanan data yang penting atau data yang bersifat rahasia yaitu kerahasiaan data, keabsahan dan ketersediaan data. menjaga data dari berbagai serang pihak yang tidak berkepentingan [1].

Teknik kriptografi memiliki berbagai algoritma yang dapat digunakan untuk melakukan fungsinya dalam mengamankan data. Secara umum kekuatan dari algoritma kriptografi tidak selamanya terletak

pada rumitnya pemecahan sebuah algoritma, namun kekuatan algoritma terletak pada kunci yang digunakan sebagai elemen dari algoritma itu sendiri. Semakin rumit proses pembentukan kunci pada sebuah algoritma kriptografi akan berdampak terhadap keoptimalan algoritma itu sendiri. Berdasarkan penelitian terdahulu, mengatakan bahwa kerahasiaan serta prosedur pembentukan kunci merupakan salah satu aspek penting dalam mengimplementasikan teknik keamanan data. Semakin rahasia dan rumitnya pembentukan kunci yang digunakan, maka semakin baik dan optimal algoritma keamanan data yang digunakan [2].

Salah satu algoritma kriptografi yang dapat digunakan untuk mengamankan data adalah *beafort cipher*. *Beaufort cipher* merupakan pengembangan dari *vegenere cipher* dan termasuk dalam algoritma kunci simetri, sehingga cara kerja algoritma ini sama dengan algoritma *vegenere cipher*. Proses enkripsi maupun dekripsi menggunakan karakter kunci dengan jumlah yang sama dengan jumlah karakter data asli (*plain*), karena pada algoritma ini masing-masing karakter data asli harus berpasangan dengan masing-masing karakter kunci. Bila karakter kunci lebih pendek dari jumlah karakter data yang akan diamankan, maka akan dilakukan pengulangan kata kunci hingga jumlahnya sama dengan jumlah data asli. Hal inilah yang menyebabkan para pengguna sulit untuk menghafal kata kunci yang terlalu panjang. Berdasarkan penelitian terdahulu mengatakan bahwa penggunaan kata kunci secara berulang sangat rentang dan sangat mudah dipecahkan oleh penyerang, sehingga penggunaan kunci seperti ini sangat tidak disarankan untuk digunakan dalam pengaman data [3].

Salah satu teknik pembangkitan bilangan acak adalah algoritma freivalds dimana algoritma ini mampu melakukan pembangkitan bilangan acak berdasarkan proses pengacakan matrix dengan probabilitas yang sangat tinggi. Berdasarkan penelitian terdahulu, mengatakan bahwa algoritma freivalds ini mampu mengurangi batas waktu proses dengan probabilitas yang sangat tinggi sehingga dapat berjalan di $0(n^{2.379})$ waktu [4].

Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk membangkitkan kunci yang digunakan pada *beaufort cipher* untuk mengenkripsi dan dekripsi data teks. Proses pembangkitan kunci dilakukan berdasarkan algoritma freivalds, sehingga kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang dibangkitkan berdasarkan algoritma ini. Implementasi algoritma ini diharapkan dapat mengoptimalkan kekuatan algoritma *beufort cipher* yang sangat tergantung pada kekuatan kunci yang digunakan, sehingga data yang diamankan tidak mudah dipecahkan oleh pihak yang tidak bertanggung jawab.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Adapun langkah-langkah yang dilakukan dalam menyelesaikan penelitian ini dimulai dari proses identifikasi masalah keamanan data, melakukan studi leteratur dari berbagai sumber baik buku maupun jurnal, analisa algoritma *beaufort cipher*, pembangkitan kunci *beaufort cipher* berdasarkan algoritma *freivalds*, pembahasan, implementasi dalam bentuk contoh kasus serta kesimpulan. Langkah-langkah tersebut disajikan dalam bentuk kerangka penelitian seperti yang diperlihatkan pada gambar 1.

Gambar 1. Tahap-tahap Penelitian

Bedasarkan gambar 1 di atas, dapat dijelaskan langkah-langkah dalam menyelesaikan penelitian in adalah :

1. Identifikasi Masalah
   Langkah ini merupakan langkah yang mengawali penelitian ini, dimana pada langkah ini merupakan identifikasi terhadap permasalahan keamanan data teks dan identifikasi kekuatan algoritma yang digunakan dalam penerapan teknik pengamanan data.
2. Studi Pustaka
   Langkah ini merupakan langkah yang penting dilakukan untuk mengetahui teori-teori yang relevan dengan masalah yang telah teridentifikasi yang dapat bersumber dari buku maupun jurnal-jurnal ilmiah yang relevan.
3. Analisa Algoritma *Beaufort Cipher* dan *Freivalds*

Langkah ini merupakan penguraian analisa terhadap cara kerja *beaufort cipher* terutama analisa terhadap kelemahan dalam proses pembangkitan kunci serta analisa terhadap penerapan algoritma *freivalds*.

4. Pembahasan
   Langkah ini merupakan penguraian prosedur pembangkitan kunci algoritma *beaufort cipher* berdasarkan algoritma *freivalds*
5. Implementasi
   Langkah ini merupakan penguraian prosedur penerapan pengamanan data teks berdasarkan algoritma beaufort cipher dengan kata kunci yang dibangkitkan berdasarkan algoritma freivalds
6. Kesimpulan
   Merupakan langkah yang dilakukan untuk menyimpulkan hasil dari penelitian ini, termasuk pengujian yang dilakukan.

2.2 Kriptografi

Salah satu teknik yang umum digunakan dalam mengamankan data yang sifatnya rahasia atau pribadi adalah teknik kriptografi. Defenisi lain dari kriptografi merupakan salah satu teknik yang mempelajari agar pesan yang disitribusikan kepada orang lain dapat sampaikan dengan aman [5]. Beberapa hal yang harus dicapai dalam mengimplementasikan kriptografi, adalah kerahasiaan (*confidentiality*), integritas data (data *integrity*), autentikasi (*authentication*), ketiadaan penyangkalan (*nonrepudiation*) [6]. Ada tiga fungsi utama dari teknik kriptografi yaitu enkripsi, dekripsi dan kunci [7].

Beberapa kekuatan yang dimiliki oleh algoritma kriptografi dalam proses mengenkripsi data [8], yaitu:

1. Konfusi/pembingungan (*confusion*), yaitu suatu proses dimana teks sulit dikembalikan pada bentuk awal secara tanpa melalui proses dekripsi.
2. Difusi/peleburan *(difusion*), yaitu suatu proses dimana karakteristik suatu teks dihilangkan sehingga mengamankan suatu informasi.

2.3 Algoritma Beaufort Cipher

Algoritma ini termasuk dalam ke dalam kelompok kriptografi klasik dimana kunci (K) pada *beaufort cipher* adalah urutan karakter-karakter $K = k1 \ldots k_d$. Nilai $k1$ merupakan nilai atau jumlah pergeseran dari alfabet ke-*i* [9]. Sehingga dapat diartikan bahwa jumlah karakter kunci yang digunakan berbanding lurus dengan jumlah karakter plain yang ingin diamankan, sehingga masing-masing karakter plain harus memiliki pasangan kunci. Hal ini yang menyebabkan algoritma ini hampir sama dengan algoritma *vigeneere cipher*. Adapun formulasi yang digunakan dalam proses enkripsi dan dekripsi [10], adalah :

Formula proses enkripsi :

$$Ci = Ek(Mi) = (Ki + Mi) \text{ Mod } 26 \quad (1)$$

Formula proses dekripsi :

$$Mi = Dk(Ci) = (Ki - Mi) \text{ Mod } 26 \quad (2)$$

Keterangan :

Mi = Elemen data yang diamankan
Ci = Cipher Ki = Kunci
Ek = Fungsi Enkripsi Dk = Fungsi Dekripsi

Agar seluruh nilai ASCI dapat diakses di dalam komputer, maka nilai modulus dapat diganti dengan 256.

2.4 Algoritma Freivalds

Secara sederhana algoritma freivalds dapat didefenisikan sebagai sebuah algoritma deterministik yang dapat membangkitkan bilangan acak dengan memanfaatkan probablitas yang sangat tinggi yang diperoleh berdasarkan operasi matrix. Algoritma ini akan melakukan verifikasi hasil operasi matix terhadap input yang diberikan yang dinyatakan dengan A x B = C. Input yang diberikan adalah bilangan-bilangan bulat dan mampu memverifikasi kebenaran input dan hasil matrix lebih cepat daripada melakukan perhitungan ulang [4] [11].

Agar wakru yang dibutuhkan dapat lebih sedikit, maka algoritma ini menerapkan teknik pengacakan dengan probabilitas tinggi. Adapun langkah-langkah yang dilakukan untuk menerapkan lagoritma ini [12] [13],adalah :

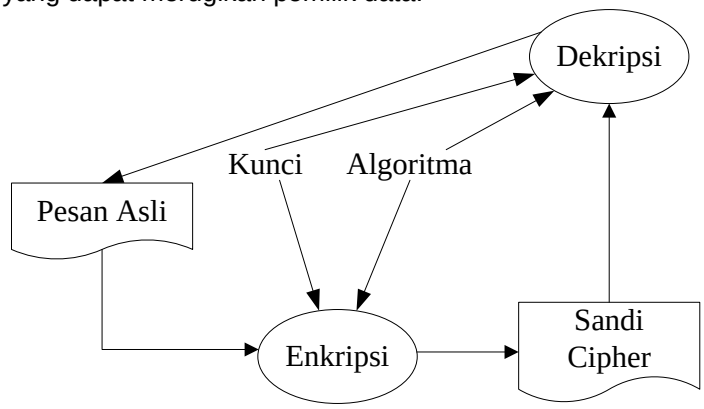
1. Hasilkan vector n/1, acak 0/1
2. Hitung nilai P = A x (Br)-Cr

dimana :

P = Hasil Pengacakan
r = Nilai vector pengacakan
A = Variable acak nilai matrix A
B = Variabel acak nilai matrix B
C = Hasil perkalian matrix A dan B

3. HASIL DAN ANALISIS

Permasalah keamanan data memang menjadi salah satu masalah penting yang harus diperhatikan pada perkembangan teknologi saat ini. Sangat banyak kasus yang terjadi saat ini terkait dengan keamanan data penting, misalnya pencurian data, manipulasi data, pemalsuan data dan tindakan lain yang menyebabkan kerugian sendiri bagi pemilik maupun penerima data. Teknik kriptografi merupakan salah satu teknik pengamanan data yang sifatnya penting. Teknik kriptografi bekerja dengan melakukan mengubah data asli menjadi sandi-sandi yang tidak dapat lagi mendeskripsikan pola dan makna asli dari data yang sebenarnya. Pemanfaatan teknik ini dapat meminimalisir kemudahan bagi orang lain yang tidak berhak mengakses data penting atau rahasia untuk melakukan tindakan-tindakan pencurian, manipulasi maupun penggunaan informasi tersebut untuk tujuan tertentu yang dapat merugikan pemilik data.



Gambar 2. Skema Pengamanan Pesan Berdasarkan Teknik Kriptogafi

Algoritma kriptografi yang bersifat umum (*public*), telah memberikan keleluasaan bagi para pengembang maupun para penyerang untuk mencari celah pemecahan dari berbagai algoritma kriptografi yang umum digunakan dalam mengamankan data, termasuk algoritma *beaufort cipher*. Hal ini jugalah yang menyebabkan lahirnya pemutakhiran atau perbaikan terhadap berbagai algoritma kriptografi agar tetap berfungsi sebagai salah satu alternatif algoritma yang dapat dihandalkan untuk mengamankan data. Pengembangan yang dilakukan bertujuan untuk mengoptimalkan kinerja sebuah algoritma untuk mencapai tujuan utama dari kriptografi yaitu *confusion* dan *diffusion*.

3.1 Pembangkitan Kunci Beaufort Cipher Berdasarkan Freivalds

Algoritma *beaufort cipher* memiliki cara kerja yang hampir sama dengan cara kerja algoritma *vegener cipher* untuk menyandikan data penting. Algoritma ini memanfaatkan teknik subtitusi (penggantian karakter) untuk mendapatkan sandi dari data asli. Agar didapatkan karakter hasil subtitusi, algoritma ini memanfaatkan nilai-nilai kunci yang ditambahkan dengan nilai dari masing-masing karakter yang disandikan. Umumnya kata kunci yang digunakan adalah kata-kata yang umum digunakan sehari-hari. Jumlah karakter kunci pada algoritma ini harus sama jumlanya dengan banyaknya karakter data asli.

Salah satu kelemahan dari algoritma ini adalah penggunaan kunci secara berulang hingga jumlahnya sama dengan jumlah karakter data asli, sehingga bila ditemukan kata kunci yang benar, maka penyerang hanya mengulang kata-kata kunci tersebut hingga jumlah karakternya sama dengan jumlah karakter sandi. Inilah salah satu alasan kenapa algoritma ini disebut hanya bergantung pada pola *confussion* untuk mendapatkan *cipher*.

Penelitian ini akan menguraikan bagaimana mengoptimalkan kunci yang digunakan pada proses enkripsi dan dekripsi. Pengoptimalan yang dilakukan adalah membangkitkan karakter-karakter kunci secara acak berdasarkan prosedur pembangkit kunci *freivalds*. Hal ini dilakukan agar kunci enkripsi maupun kunci dektipri berdasarkan algoritma *beaufort cipher* jauh lebih rumit untuk dipecahkan dan diketahui oleh penyerang. Adapun skema modifikasi kunci pada algoritma vegeneere cipher ditunjukkan pada diagaram di bawah ini :

Gambar 3. Skema Modifikasi Kunci *Beaufort Cipher*

Proses pembangkitan kunci berdasarkan algoritma *freivalds* dilakukan untuk mendapatkan beberapa bilangan acak yang dapat digunakan untuk menelengkapi kata kunci yang masih kurang pada algoritma *baufort cipher*. Bila dimisalkan kata kunci awal yang diberikan hanya sebanyak 6 karakter dan tidak memenuhi jumlah karakter teks yang akan diamankan, sehingga sisanya dapat dicari dengan memanfaatkan perkalian matrix ordo 3x3 agar kata kunci yang menjadi sisanya didapatkan sehingga sesuai dengan jumlah elemen dari data teks yang diamanakan berdasarkan konsep *beaufort cipher*, sehingga nilai-nilai kunci yang dihasilkan benar-benar acak dan *diffusion*.

3.2 Penerapan Dalam Pengamana Data Teks

Proses pembangkitan kunci berdasarkan algoritma freivalds dalam penelitian ini akan diimplementasikan dalam proses pembangkitan untuk melakukan proses enkripsi dan dekripsi 9 karakter teks yaitu BUDIDARMA dengan kata kunci ABC123. Berdsarkan jumlah karakter kunci, maka diketahui bahwa semua karakter teks yang akan diamankan tidak memiliki pasangat kunci, karena jumlah karakter kunci lebih sedikit daripada jumlah karakter teks yang akan diamankan. Oleh kerena itu, maka perlu dilakukan pencarian karakter kunci sehingga jumlah karakter kunci sama dengan jumlah karakter teks yang akan diamankan. Proses pembangkitan karakter kunci yang masih kurang tersebut dilakukan berdasarkan algoritma freivalds.

Palintext = BUDIDARMA
Kunci = ABC123

Proses pembangkitan kunci berdasarkan algoritma freivalds :

$$r = \begin{bmatrix}1\\1\\1\end{bmatrix}$$

$$A = \begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} \text{ dan } B = \begin{bmatrix}3 & 5 & 11\\5 & 11 & 2\\11 & 3 & 5\end{bmatrix}$$

P = A x (Br)-C $\begin{bmatrix}1\\0\\1\end{bmatrix}$

$$C = \begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} x \begin{bmatrix}3 & 5 & 11\\5 & 11 & 2\\11 & 3 & 5\end{bmatrix}$$

$$C = \begin{bmatrix}224 & 127 & 134\\138 & 208 & 130\\144 & 105 & 198\end{bmatrix}$$

Sehingga proses untuk mendapatkan nilai P adalah :

$$P = \begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} x \left(\begin{bmatrix}3 & 5 & 11\\5 & 11 & 2\\11 & 3 & 5\end{bmatrix} x \begin{bmatrix}1\\1\\1\end{bmatrix}\right) - \left(\begin{bmatrix}3 & 5 & 11\\5 & 11 & 2\\11 & 3 & 5\end{bmatrix} x \begin{bmatrix}1\\0\\1\end{bmatrix}\right)$$

$$P = \begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} x \begin{bmatrix}3 & +5 & +11\\7 & +13 & +3\\13 & +2 & +7\end{bmatrix} - \begin{bmatrix}224 & 0 & 134\\138 & 0 & 130\\144 & 0 & 198\end{bmatrix}$$

$$P = \begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} x \begin{bmatrix}19\\23\\22\end{bmatrix} - \begin{bmatrix}358\\268\\342\end{bmatrix}$$

$$P = \begin{bmatrix}485\\476\\447\end{bmatrix} - \begin{bmatrix}358\\268\\342\end{bmatrix}$$

$P = \begin{bmatrix}127\\208\\105\end{bmatrix}$ dirubah ke dalam bentuk karakter, menjadi $\begin{bmatrix}□\\Ì\\ą\end{bmatrix}$

Nilai matrix P inilah yang akan digunakan sebagai nilai karakter kunci yang digunakan untuk melengkpai karakter kunci yang masih kekurangan sebelumnya. Sehingga karakter-karakter kunci menjadi:

Text =	B	U	D	I	D	A	R	M	A
Key =	A	B	C	1	2	3	□	Ì	ą

Setelah masing-masing karakter teks yang akan diamankan telah dilengkapi dengan karakter kunci pasangannya masing-masing, maka proses enkripsi dan dekripsi dilakukan berdasarkan *beaufort cipher*.

Proses enkripsi :
Agar proses enkripsi lebih jelas, maka masing-masing karakter teks maupun kunci dirubah ke dalam bentuk nilai decimal, sehingga dihatilkan :

Text =	B	U	D	I	D	A	R	M	A
Decimal	66	85	68	73	68	65	82	77	65
Key =	A	B	C	1	2	3	□	Ì	ą
Decimal	65	66	67	49	50	51	127	208	105

Formula yang digunakan untuk mengenkripsi adalah (Ki-Mi) mod 256. Modulus 256 digunakan agar semua karakter yang dihasilkan merupakan karakter yang dikenali dan ada didalam tabel ASCII.

Desimal Key (K)	=	65	66	67	49	50	51	127	208	105
Desimal Teks (M)	=	66	85	68	73	68	65	82	77	65
(Ki+Mi) Mod 256	=	131	151	135	122	118	116	209	29	170
Char Cipher	=	ƒ	—	‡	z	v	t	Ñ		ª

Berdasarkan proses di atas, maka dihasilkan *cipher* dari teks BUDIDARMA adalah ƒ—‡zvtÑ

Proses dekripsi (pengembalian *ciphertext* menjadi teks asli) dilakukan dengan cara yang sama seperti di atas, hanya saja formulasi yang digunakan adalah melakukan operasi pengurangan antara nilai decimal *cipher* dengan nilai decimal kunci. Kunci yang digunakan pada proses dekripsi adalah kunci yang sama seperti yang digunakan pada proses enkripsi. Proses pembangkitan kunci yang kurang tetap dilakukan seperti pada proses pembangkitan kunci berdasarkan algoritma *freivalds*.

Cipher : ƒ — ‡ z v t Ñ ª

Bila dikonversi ke decimal :

Char Cipher	=	ƒ	—	‡	z	v	t	Ñ		ª
Desimal Key (K)	=	65	66	67	49	50	51	127	208	105
Desimal Cipher (M)	=	131	151	135	122	118	116	209	29	170
(Ki-Mi) Mod 256	=	66	85	68	73	68	65	82	77	65
Char Cipher	=	B	U	D	I	D	A	R	M	A

4. KESIMPULAN

Berdasarkan uraian penelitian di atas, maka dapat disimpulkan bahwa:

1. Pemanfaatan algoritma pembangkit nilai acak untuk menghasilkan nilai-nilai kunci pada algoritma kriptografi dapat dilakukan untuk mengiptimalkan ketahanan dari sebuah algoritma kriptografi dari tindakan penyerangan.
2. Pembangkitan kunci berdasarkan algoritma *freivalds cipher* dapat menghasilkan nilai-nilai kunci yang tidak berulang, sehingga dapat mengoptimalkan ketahanan kunci *beaufort cipher*
3. Perlu dilakukan modifikasi pembentukan kunci pada algoritma kriptografi klasik untuk meningkatkan keoptimalan ketahanannya terhadap serangan

REFERENSI

[1] M. Fachry, . A. Kusyanti and K. Amron, "Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 2, no. 11, pp. 4863-4869, 2018.

[2] C. Irawan and E. H. Rachmawanto, "Implementasi Kriptografi dengan Menggunakan Algoritma Arnold's Cat Map dan Henon Map," *Jurnal Masyarakat Informatika ,* vol. 13, no. 1, pp. 15-32, 2022.

[3] B. O. Sinaga, S. Sinurat and T. Zebua, "Modifikasi Algoritma XTEA dengan Pembangkitan Kunci Menggunakan Metode Linear Congruential Untuk Pengamanan File Dokumen," *Journal of Informatics Management and Information Technology,* vol. 1, no. 4, pp. 144-152, 2021.

[4] R. Rahmansyah, "Penerapan Algoritma Friefalds Untuk Pembangkit Kunci Algoritma Knapsack Pada Pengamanan Record Database," *Kajian Ilmiah Informatika dan Komputer,* vol. 2, no. 4, pp. 132-137, 2022.

[5] A. Thahara and I. T. Siregar, "Implementasi Kriptografi untuk Keamanan Data dan Jaringan menggunakan Algoritma DES," *JURTI,* vol. 5, no. 1, pp. 31-38, 2021.

[6] F. Febriyanto, "Rancang Bangun Website Kriptografi Untuk Pengamanan File Gambar Digital," *JURNAL KHATULISTIWA INFORMATIKA,* vol. 2, no. 10, pp. 113 - 118, 2022.

[7] A. T. F. Alhamdi and R. F. Siahaan, "Penerapan Kriptografi Dalam Pengamanan Pesan Text Berbasis Android DenganMenggunakan Metode Rijndael," *Jurnal Mahajana Informasi,* vol. 6, no. 2, pp. 69-74, 2021.

[8] A. i. P. R. Tarigan, P. S. Ramadhan and K. Ibnutama, "Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard)," *JURNAL CYBER TECH STMIK TRIGUNA DHARMA,* vol. 5, no. 1, pp. 26-35, 2023.

[9] C. Irawan, . E. H. Rachmawanto, C. A. Sari and C. A. Sugianto, "SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM," in *Seminar Nasional LPPM – Universitas Muhammadiyah Purwokerto*, Purwokerto, 2020.

[10] A. Rachmadsyah, A. Perdana and A. Budiman, "Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks Berbasis Mobile Application," *Jurnal Minfo Polgan,* vol. 9, no. 2, pp. 12-17, 2020.

[11] H. Ji, M. Mascagni and Y. Li, "Gaussian Variant of Freivalds' Algorithm for Efficient and Reliable Matrix Product Verification," *Monte Carlo Methods and Applications,* pp. 1-7, May 2017.

[12] A. Syahputra, "Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video," *Pelita Informatika,* vol. 10, no. 2, pp. 70-77, 2021.

[13] R. Solin and . P. Ramadhani, "Modifikasi Pembangkit Kunci Algoritma Elgamal Dengan Menerapkan Algoritma Freivalds," in *Konferensi Nasional Teknologi Informasi dan Komputer)*, Medan, 2020.