JISTech (Journal of Islamic Science and Technology)

JISTech, 9(2), 146-156, July - December 2024

ISSN: 2528-5718

http://jurnal.uinsu.ac.id/index.php/jistech

Kombinasi Algoritma *Beaufort Chiper* dan *Hill Chiper* Dalam Mengamankan *File* Dokumen Berbasis Mobile

Muhaimi Rizki Siregar[1], Heri Santoso[2], Aidil Halim Lubis[3]

[1,2,3] *Universitas Islam Negeri Sumatera Utara, Medan, Indonesia*

ABSTRAK

Penelitian ini bertujuan untuk mengamankan suatu *file* dokumen yang memiliki informasi yang bersifat rahasia atau pribadi. Sehingga dibutuhkan suatu sistem yang dapat digunakan untuk mengamankan *file* dokumen sehingga tidak dapat diakses oleh orang lain yang tidak berkepentingan. Pengamanan *file* dokumen dilakukan menggunakan kombinasi algoritma beaufort cipher dan hill cipher. Beaufort cipher adalah salah satu varian dari vigenèrecipher di mana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada vigenèrecipher. HillCipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi dari aritmatika modulo. Langkah awal pengamanan dilakukan menggunakan algoritma Beaufort Cipher selanjutnya hasil pengamanan algoritma Beaufort Cipher diamankan kembali menggunakan hill cipher. Proses pengamanan dilakukan menggunakan 4 buah kunci dikarenakan hill cipher menggunakan perkalian matrix 2x2. Hasil akhir dari penelitian ini merupakan sebuah aplikasi berbasis android yang dapat digunakan dalam proses pengamanan file dokumen dengan ekstensi .docx, .xlsx dan .pdf. File dokumen yang telah diamankan akan memliki ekstensi .mhi sebagai penanda bagi peneliti. Dokumen yang telah diamankan dapat dikembalikan ke dalam bentuk aslinya menggunakan aplikasi yang telah dihasilkan pada penelitian ini menggunakan kunci yang sama digunakan dalam proses pengamanan.

ABSTRACT

This study aims to secure a document file that has confidential or private information. So we need a system that can be used to secure document files so that they cannot be accessed by unauthorized persons. Document file security is carried out using a combination of the Beaufort cipher and hill cipher algorithms. Beaufort cipher is a variant of the vigenre cipher where the encryption and decryption method is almost the same as encrypting and decrypting the vigenre cipher. Hill Cipher is a cryptographic algorithm that uses a matrix as a key to encrypt and decrypt modulo arithmetic. The initial step of security is carried out using the Beaufort Cipher algorithm, then the results of the Beaufort Cipher algorithm are secured again using Hill Cipher. The security process is carried out using 4 keys because Hill Cipher uses a 2x2 matrix multiplication. The final result of this research is an android-based application that can be used in the process of securing document files with .docx, .xlsx and .pdf extensions. Document files that have been secured will have an .mhi extension as a marker for researchers. Documents that have been secured can be returned to their original form using the application that has been generated in this study using the same key used in the security process.

Kata kunci: File Dokumen, *Beaufort Cipher, Hill Cipher*
Email Address: [1] muhaimirizki9@gmail.com, [2] herisantoso@uinsu.ac.id, [3] aidilhalimlubis@uinsu.ac.id

DOI: http://dx.doi.org/10.30829/jistech.v9i2.22633
Received 20 September 2024; Received in revised form 14 November 2024; Accepted 17 December 2024

Pendahuluan

Di dalam kehidupan sehari-hari terkadang seseorang memerlukan sistem keamanan dalam berinteraksi dengan orang lain. Sistem keamanan tersebut bertujuan untuk mencegah tindakan pencurian informasi yang bersifat rahasia. Pada saat ini teknik yang dapat digunakan untuk mengamankan suatu data adalah teknik kriptografi. Kriptografi adalah suatu teknik pengamanan data dengan melakukan perhitungan matematika antara data dengan kunci yang digunakan untuk mengubah suatu data ke dalam bentuk lain yang tidak dapat dibaca.

Sehingga hanya pemilik kunci saja yang dapat merubah kembali data ke bentuk aslinya agar informasi yang terdapat di dalamnya dapat dibaca.

Segala sesuatu yang melanggar privasi dapat diartikan sebagai tindakan pengambilan, pengubahan, atau pengaksesan terhadap data pribadi seseorang tanpa izin terlebih dahulu dari pemiliknya. Hal itu termasuk dalam kategori kejahatan *cyber*. *Cybercrime* adalah istilah yang dipakai untuk mendeskripsikan kegiatan kejahatan yang memakai media komputer maupun internet. Kegiatan-kegiatan kejahatan ini sudah mempunyai hukum yang mana di negara-negara masih sebagian terdapat perdebatan mengenai bentuk dan status hukumnya. Pengertian ini dapat didefinisikan bahwa *cybercrime* suatu aktivitas yang menggunakan komputer atau internet sebagai media atau tujuan kejahatan [1]. Islam telah mengatur dengan jelas tentang pentingnya menjaga privasi seseorang. Di dalam QS. An-Nur ayat 27 disebutkan:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Yang artinya : "Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu selalu ingat". Ayat tersebut menjelaskan pentingnya dalam menjaga suatu privasi. Pada penelitian ini yang dimaksud sebagai privasi adalah informasi rahasia yang terkandung di dalam sebuah *file* dokumen, sehingga dibutuhkan suatu cara agar dapat melindungi informasi tersebut.

Seiring berkembangnya waktu, banyak algoritma-algoritma yang menerapkan teknik kriptografi untuk digunakan dalam proses pengamanan data diantaranya adalah algoritma beaufort cipher dan algoritma hill cipher. Beaufort cipher adalah salah satu varian dari vigenère cipher di mana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada vigenère cipher. Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi dari aritmatika modulo. Setiap karakter pada plainteks ataupun cipherteks di konversikan ke dalam bentuk angka.

Penelitian ini bertujuan untuk mengamankan suatu *file* dokumen yang memiliki informasi yang bersifat rahasia atau pribadi. Sehingga dibutuhkan suatu sistem yang dapat digunakan untuk mengamankan *file* dokumen sehingga tidak dapat diakses oleh orang lain yang tidak berkepentingan. Untuk itu pada penelitian ini akan dikombinasikan algoritma beaufort cipher dan hill cipher ke dalam sebuah sistem untuk mengamankan *file* dokumen. Penggunaan dua algoritma kriptografi dalam mengamankan *file* dokumen bertujuan untuk menghasilkan tingkat keamanan yang lebih baik dalam mengamankan sebuah *file* dokumen. Sehingga *file* dokumen yang telah diamankan tidak dapat dijebol dengan mudah oleh para kriptanalisis.

Berdasarkan latar belakang di atas, maka dalam penelitian ini akan dibangun sebuah aplikasi yang dapat digunakan untuk mengamankan sebuah *file* dokumen menggunakan algoritma beaufort cipher dan hill cipher. Aplikasi keamanan *file* dokumen pada penelitian ini akan dibangun berbasis *mobile* dengan tujuan agar dapat digunakan secara mudah dan efisien dengan memanfaatkan *smartphone* android.

Kriptografi berasal dari bahasa Yunani yaitu dari dua suku kata *Crypto* dan *Graphia*. *Crypto* artinya menyembunyikan, sedangkan *graphia* artinya ilmu. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data, yang dilakukan oleh seorang Kriptographer. Kriptography berarti "secret writing" (Tulisan Rahasia). Definisi yang dipakai ini mengutip definisi yang dikemukakan Bruce Scneier dalam bukunya Applied Cryptograpy (1996), Kriptography adalah ilmu dan seni untuk menjaga keamanan pesan (Cryptografi is the art and science of keeping messages secure). Sebagai pembanding pengertian di atas Rinaldi Munir juga mengutip definisi yang dikemukakan oleh Alfret JMenezes,Paul C van Oorschot dan Scott A. Vanston dalam bukunya Handbook of applied Cryptography (1996), Kriptography adalah ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentikasi. Julius Caesar melakukan penggeseran huruf alphabet dengan mengganti semua huruf alphabet dari a, b, c, d, dengan a menjadi d, b menjadi e, c menjadi f, dan seterusnya.[2].

Beaufort cipher adalah salah satu varian dari vigenere cipher di mana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada vigenere cipher. Beaufort cipher ditemukan oleh Laksamana Sir Francis Beaufort, Royal Navy, yang juga pencipta skala beaufort, yang merupakan instrumen ahli meteorologi digunakan untuk menunjukkan kecepatan angin. Lebih rinci perbedaan dari kedua metode ini adalah peranan kunci, dalam vigenere cipher digunakan sebagai penambah *plain* teks dan pengurang cipher teks.

Sedangkan dalam formula yang digunakan beaufort cipher, kunci digunakan untuk dikurangkan dengan plain teks maupun cipher teks. Untuk lebih jelas dapat diperhatikan rumus enkripsi dan dekripsi beaufort cipher sebagai berikut:

$Cc = (k-Pc) \bmod 26$

$Pc = (k-Cc) \bmod 26$

Keterangan:
C: memodelkan ciphertext
P: memodelkan plaintext
K: memodelkan kunci.[3]

Hill cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher, karena teks yang akan diprosesakan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidakdipetakan menjadi karakter yang sama pula. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Hill Cipher diciptakan oleh Lester S.Hill pada tahun 1929. Hill Cipher tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas *plaintext*. Teknik kriptanalisis ini disebut known- plaintext attack.[4]

Java adalah bahasa pemrograman yang popular, dikembangkan oleh SunMicrosystems. Salah satu penggunaan terbesar Java adalah dalam pembuatan aplikasi *native* untuk Android. Bahasa pemrograman ini bersifat *multiplatform* yakni bahasa ini dapat digunakan di berbagai *platform*, seperti *desktop*, *android* dan bahkan untuk sistem operasi *Linux*. Sedangkan Java bersifat neutral *architecture*, karena Java *Compiler* yang digunakan untuk mengkompilasi kode program Java dirancang untuk menghasilkan kode yang netral terhadap semua arsitektur perangkat keras yang disebut sebagai Java *Bytecode*. [5]

Android merupakan sistem operasi berbasis Linux yang digunakan untuk telepon seluler (*mobile*) seperti telepon pintar (*smartphone*) dan komputer tablet (PDA). Android adalah sebuah sistem operasi untuk perangkat *mobile* berbasis Linux yang mencangkup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri yang akan digunakan untuk membantu kegiatan dalam berbagai bidang, sehingga bisa digunakan oleh setiap orang yang ingin menggunakannya pada perangkat mereka.Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat bergerak layar sentuh seperti telepon pintar dan komputer tablet. Android awalnya dikembangkan oleh Android, Inc dengan dukungan finansial Google, yang kemudian membelinya pada tahun 2005. [6]

Android Studio merupakan lingkungan pengembangan perangkat lunak terpadu *Integrated Development Environment* (IDE) untuk pengembangan aplikasi Android, berdasarkan Intellij IDEA. Selain merupakan editor kode Intellij dan alat pengembang yang berdaya guna, Android Studio juga menawarkan banyak fitur untuk meningkatkan produktivitas saat membuat aplikasi Android. Android studio sendiri dikembangkan berdasarkan Intellij IDEA yang mirip dengan Eclipse disertai dengan ADT plugin (Android Development Tools). Android Studio memiliki fitur:

a. Projek berbasis pada Gradle Build
b. Refactory dan pembenahan bug yang cepat
c. Tools baru yang bernama "Lint" diklaim dapat memonitor kecepatan, kegunaan, serta kompetibelitas aplikasi dengan cepat.
d. Mendukung Proguard And App-signing untuk keamanan.
e. Memiliki GUI aplikasi android lebih mudah
f. Didukung oleh Google Cloud Platfrom untuk setiap aplikasi yang dikembangkan [6].

Android SDK mencakup perangkat *tools* pengembangan yang komprehensif. Android SDK terdiri dari *debugger*, *libraries*, *handsetemulator*, dokumentasi, contoh kode program dan tutorial. Saat ini Android sudah mendukung arsitektur x86 pada Linux (distribusi Linux apapun untuk desktop modern), Mac OS X 10.4.8 atau lebih, Windows XP atau Vista. Persyaratan mencakup JDK, Apache Ant dan Python 2.2 atau lebih. *IDE* yang didukung secara resmi adalah *Eclipse* 3.2 atau lebih dengan menggunakan *plugin Android Development Tools* (*ADT*), dengan ini pengembang dapat menggunakan *IDE* untuk mengedit dokumen *Java* dan *XML* serta menggunakan peralatan *commandline* untuk menciptakan, membangun, melakukan *debug* aplikasi Android dan pengendalian perangkat Android (misalnya *reboot*, menginstal paket perangkat lunak).

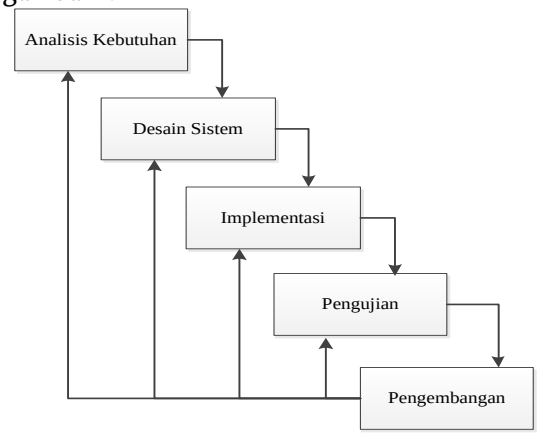
Android SDK mencakup perangkat *tools* pengembangan yang komprehensif. android SDK terdiri dari *debugger, libraries, handset emulator*, dokumentasi, dengan menggunakan *plugin Android Development Tools* (ADT), dengan ini pengembang dapat menggunakan ide untuk mengedit dokumen java dan XML serta menggunakan

peralatan command line untuk menciptakan, membangun, melakukan debug aplikasi android dan pengendalian perangkat android. [7]

Metodologi Penelitian

a. Skema Alur Penelitian

Metode penelitian yang digunakan pada penelitian ini adalah menggunakan teknik SDLC (*System Development Life Cycle*) yaitu proses logisyang digunakan oleh peneliti untuk membangun sebuah aplikasi yang dapat digunakan untuk mengamankan *file* dokumen menggunakan kombinasi algoritma beaufort cipher dan hill cipher. Langkah-langkah yang diperlukan untuk mencapai tujuan dalam penggunaan metode penelitian SDLC dapat dilihat pada model *waterfall* gambar 1.



Gambar 1. Model *Waterfall* Metode Penelitian

b. Pengumpulan Data

Sistem yang dirancang membutuhkan pengumpulan data, ada beberapa penentuan dalam proses pengumpulan data,yaitu:

1. Studi Literatur, memahami referensi dan literatur yang berkaitan tentang materi risalah. Referensi yang digunakan biasanya terkait dengan penulisan risalah di Universitas Islam Negeri Sumatera Utara, serta jurnal untuk mempelajari literatur yang digunakan untuk menulis skripsi.
2. Pengamatan, pengumpulan data dan informasi dengan mengamati secara langsung beberapa contoh aplikasi kriptografi. Contoh *script* bahasa pemograman yang diamati tersebut selanjutnya akan dituangkan ke dalam bahasa pemrograman Java yang sesuai dengan aplikasi yang akan dibangun pada penelitian ini.

c. Tahapan Enkripsi

Tahapan dari proses enkripsi adalah sebagai berikut:

1. Proses enkripsi dimulai dengan memilih *file* dokumen yang akan diamankan dan menginputkan kunci untuk proses enkripsi.
2. Selanjutnya algoritma pertama yang digunakan dalam proses enkripsi adalah algoritma beaufort.
3. Langkah berikutnya melakukan proses enkripsi kembali *file* dokumen yang telah dienkripsi menggunakan algoritma beaufort dengan algoritma hill cipher.
4. Hasil enkripsi *file* dokumen menggunakan algoritma hill cipher merupakan hasil akhir dari proses enkripsi.

d. Tahapan Dekripsi

Tahapan dari proses dekripsi adalah sebagai berikut:

1. Proses dekripsi dimulai dengan memilih *file* dokumen yang telah di enkripsi dan menginputkan kunci yang sama dengan kunci yang digunakan dalam proses enkripsi.
2. Selanjutnya sistem akan menggunakan algoritma hill cipher sebagai algoritma pertama dalam melakukan proses dekripsi.
3. Setelah selesai melakukan dekripsi menggunakan algoritma hill ciphert, selanjutnya sistem akan melakukan kembali proses dekripsi menggunakan algoritma beaufort.
4. Hasil dekripsi akhir menggunakan algoritma beaufort akan mengembalikan *file* dokumen ke dalam bentuk aslinya sehingga datanya dapat diakses.

Hasil dan Pembahasan

a. Proses Enkripsi

Plaintext : dokumen aman

Kunci : siap

Proses enkripsi yang pertama dilakukan adalah menggunakan algoritma beaufort cipher. Pada penelitian ini akan digunakan himpunan 26 karakter dalam proses enkripsi menggunakan algoritma beaufort cipher sehingga didapatkan nilai masing-masing karakter adalah :

Tabel 1. Himpunan Karakter Algoritma Beaufort Cipher

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nilai	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Karakter	O	P	Q	R	S	T	U	V	W	X	Y	Z		
Nilai	14	15	16	17	18	19	20	21	22	23	24	25		

Proses enkripsi algoritma beaufort cipher adalah sebagai berikut:

C1 = (K1 - P1) mod 26
= (s - d) mod 26
= (18 - 3) mod 26
= 15
= p

C2 = (K2 - P2) mod 26
= (i - o) mod 26
= (8 - 14) mod 26
= 20
= u

C3 = (K3 - P3) mod 26
= (a - k) mod 26
= (0 - 10) mod 26
= 16
= q

C4 = (K4 - P4) mod 26
= (p - u) mod 26
= (15 - 20) mod 26
= 21
= v

C5 = (K5 - P5) mod 26
= (s - m) mod 26
= (18 - 12) mod 26
= 6
= g

C6 = (K6 - P6) mod 26
= (i - e) mod 26
= (8 - 4) mod 26
= 4
= e

C7 = (K7 - P7) mod 26
= (a - n) mod 26
= (0 - 13) mod 26
= 13
= n

C8 = (K8 - P8) mod 26
= (p - a) mod 26
= (15 - 0) mod 26
= 15
= p

C9 = (K9 - P9) mod 26
= (s - m) mod 26
= (18 - 12) mod 26
= 6
= g

C10 = (K10 - P10) mod 26
= (i - a) mod 26
= (8 - 0) mod 26

= 8
= i

C11 = (K11 - P11) mod 26
= (a - n) mod 26
= (0 - 13) mod 26
= 13
= n

Hasil dari proses enkripsi menggunakan algoritma beaufort cipher adalah "**puqvgen pgin**". Selanjutnya dilakukan proses enkripsi menggunakan algoritma hill cipher terhadap ciphertext yang dihasilkan dari proses enkripsi menggunakan algoritma beaufort cipher. Dalam proses enkripsi menggunakan algoritma hill cipher digunakan urutan himpunan karakter sebagai berikut:

Tabel 2. Himpunan Karakter Algoritma Hill Cipher

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nilai	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Karakter	O	P	Q	R	S	T	U	V	W	X	Y	Z	a	b
Nilai	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Karakter	c	d	e	f	g	h	i	j	k	l	m	n	o	p
Nilai	28	29	30	31	32	33	34	35	36	37	38	39	40	41
Karakter	q	r	s	t	u	v	w	x	y	z	0	1	2	3
Nilai	42	43	44	45	46	47	48	49	50	51	52	53	54	55
Karakter	4	5	6	7	8	9		?	!	.	,			
Nilai	56	57	58	59	60	61	62	63	64	65	66			

Plaintext = puqvgen pgin = 41 46 42 47 32 30 39 62 41 32 34 39
Kunci = siap = 44 34 26 41

Proses enkripsi dilakukan dengan cara perhitungan matriks dengan *plaintext* dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Blok *plaintext* dienkripsi dengan kunci:

$C_{1,2} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix}\begin{bmatrix}41\\46\end{bmatrix} (mod\ 67) = \begin{bmatrix}18\\4\end{bmatrix}$ = SE

$C_{3,4} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix}\begin{bmatrix}42\\47\end{bmatrix} (mod\ 67) = \begin{bmatrix}29\\4\end{bmatrix}$ = DE

$C_{5,6} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix}\begin{bmatrix}32\\30\end{bmatrix} (mod\ 67) = \begin{bmatrix}16\\52\end{bmatrix}$ = Qo

$C_{7,8} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix}\begin{bmatrix}39\\62\end{bmatrix} (mod\ 67) = \begin{bmatrix}5\\5\end{bmatrix}$ = FF

$C_{9,10} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix}\begin{bmatrix}41\\32\end{bmatrix} (mod\ 67) = \begin{bmatrix}11\\33\end{bmatrix}$ = Lh

$C_{11,12} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix}\begin{bmatrix}34\\39\end{bmatrix} (mod\ 67) = \begin{bmatrix}8\\4\end{bmatrix}$ = IE

Hasil akhir dari proses enkripsi menggunakan kombinasi algoritma Beaufort dan Hill Cipher adalah "**SEDEQoFFLhIE**".

b. Proses Dekripsi

Proses dekripsi pertama kali dilakukan dengan menggunakan algoritma hill cipher. Tahap awal dari proses dekripsi menggunakan algoritma hill cipher adalah mencari nilai inverse dari kunci yang digunakan. Mencari invers dapat dilakukan dengan menggunakan metode operasi baris (row operation) atau metode determinan. Setelah melakukan perhitungan, didapat matriks K^{-1}yang merupakan invers dari matriks K, yaitu:

$K^{-1} = \begin{bmatrix}-6 & 54\\ 61 & -62\end{bmatrix} = \begin{bmatrix}44 & 34\\ 26 & 41\end{bmatrix} (mod\ 67)$

Sehingga didapatkan nilai kunci invers yang akan digunakan dalam proses dekripsi menggunakan algoritma hill cipher adalah -6 54 61 -62. Selanjutnya dilakukan proses dekripsi menggunakan algoritma Hill Cipher sebagai berikut:

$C_{1,2} = \begin{bmatrix}-6 & 54\\ 61 & -62\end{bmatrix}\begin{bmatrix}18\\4\end{bmatrix} (mod\ 67) = \begin{bmatrix}41\\46\end{bmatrix}$ = pu

$C_{3,4} = \begin{bmatrix}-6 & 54\\ 61 & -62\end{bmatrix}\begin{bmatrix}29\\4\end{bmatrix} (mod\ 67) = \begin{bmatrix}42\\47\end{bmatrix}$ = qv

$C_{5,6} = \begin{bmatrix}-6 & 54\\ 61 & -62\end{bmatrix}\begin{bmatrix}16\\52\end{bmatrix} (mod\ 67) = \begin{bmatrix}32\\30\end{bmatrix}$ = ge

$C_{7,8} = \begin{bmatrix}-6 & 54\\ 61 & -62\end{bmatrix}\begin{bmatrix}5\\5\end{bmatrix} (mod\ 67) = \begin{bmatrix}39\\62\end{bmatrix}$ = n

$C_{9,10} = \begin{bmatrix}-6 & 54\\ 61 & -62\end{bmatrix}\begin{bmatrix}11\\33\end{bmatrix} (mod\ 67) = \begin{bmatrix}41\\32\end{bmatrix}$ = pg

$C_{11,12}$ $= \begin{bmatrix} -6 & 54 \\ 61 & -62 \end{bmatrix} \begin{bmatrix} 8 \\ 4 \end{bmatrix} (mod\ 67) = \begin{bmatrix} 34 \\ 39 \end{bmatrix}$ = in

Hasil dekripsi yang didapat menggunakan algoritma Hill Cipher adalah "**puqvgen pgin**". Selanjutnya dilakukan kembali proses dekripsi menggunakan algoritma Beaufort sebagai berikut:

Plaintext : puqvgen pgin
Kunci : siap

P1 = (K1 - C1) mod 26
= (s - p) mod 26
= (18 - 15) mod 26
= 3
= d

P2 = (K2 - C2) mod 26
= (i - u) mod 26
= (8 - 20) mod 26
= 14
= o

P3 = (K3 - C3) mod 26
= (a - q) mod 26
= (0 - 16) mod 26
= 10
= k

P4 = (K4 - C4) mod 26
= (p - v) mod 26
= (15 - 21) mod 26
= 20
= u

P5 = (K5 - C5) mod 26
= (s - g) mod 26
= (18 - 6) mod 26
= 12
= m

P6 = (K6 - C6) mod 26
= (i - e) mod 26
= (8 - 4) mod 26
= 4
= e

P7 = (K7 - C7) mod 26
= (a - n) mod 26
= (0 - 13) mod 26
= 13
= n

P8 = (K8 - C8) mod 26
= (p - p) mod 26
= (15 - 15) mod 26
= 0
= a

P9 = (K9 - C9) mod 26
= (s - g) mod 26
= (18 - 6) mod 26
= 12
= m

P10 = (K10 - C10) mod 26
= (i - i) mod 26
= (8 - 8) mod 26

= 0
= a

P11 = (K11 - C11) mod 26
= (a - n) mod 26
= (0 - 13) mod 26
= 13
= n

Dari proses dekripsi menggunakan algoritma Beaufort didapatkan hasil akhir *plaintext* berupa "**dokumen aman**".

c. Tampilan Aplikasi

Berikut ini merupakan hasil pengujian aplikasi saat dijalankan pada perangkat *mobile* dengan sistem operasi android. Hasil pengujian dari masing-masing halaman dapat dilihat sebagai berikut:

1. Tampilan Halaman Utama
   Halaman utama merupakan halaman yang akan tampil pertama saat aplikasi dijalankan pada perangkat *mobile*. Halaman utama dari aplikasi dapat dilihat pada gambar 2 sebagai berikut:

Gambar 2. Tampilan Halaman Utama

2. Tampilan Halaman Enkripsi Dokumen
   Menu enkripsi dokumen digunakan untuk menampilkan halaman enkripsi *file* dokumen. Halaman enkripsi *file* dokumen digunakan dalam proses enkripsi *file* dokumen. Tampilan halaman enkripsi dokumen dapat dilihat pada gambar 3.

Gambar 3. Tampilan Halaman Enkripsi Dokumen

3. Tampilan Halaman Dekripsi Dokumen
   Menu dekripsi dokumen digunakan untuk menampilkan halaman dekripsi *file* dokumen. Pada halaman ini pengguna dapat melakukan proses dekripsi *file* dokumen. Tampilan halaman dekripsi *file* dokumen dapat dilihat pada gambar 4.

Gambar 4. Tampilan Halaman Dekripsi Dokumen

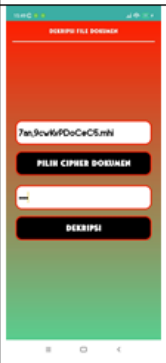
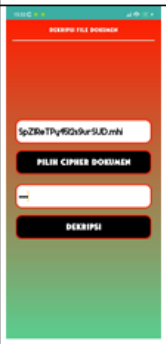
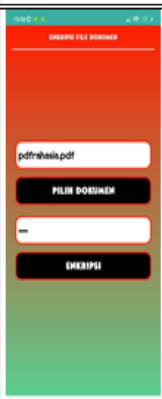
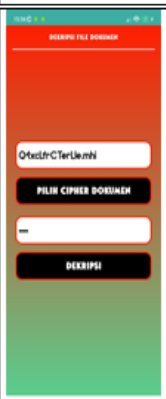
4. Tampilan Halaman Tentang Aplikasi
   Halaman tentang aplikasi menampilkan informasi dari pelaksana penelitian. Tampilan halaman tentang aplikasi pada aplikasi dapat dilihat pada gambar 5.

Gambar 5. Tampilan Halaman Tentang Aplikasi

d. Hasil Pengujian Aplikasi

Dalam pengujian penelitian akan melakukan proses enkripsi dan dekripsi beberapa dokumen word, dokumen excel, dan dokumen PDF. Hasil pengujian dapat dilihat pada tabel 3.

Tabel 3. Hasil Pengujian Aplikasi

No.	Enkripsi	Dekripsi	Keterangan
1			Ukuran awal file : 12,49 KB Plaintext : dokumenword.docx Kunci : okey Ciphertext : 7an,9cwKvPDoCeC5.mhi Ukuran akhir file : 12,5 KB
2			Ukuran awal file : 8,71 KB Plaintext : pengamananexcel.xlsx Kunci : siap Ciphertext : SpZlReTPy4512s9urSUD.mhi Ukuran akhir file : 8,71 KB
3			Ukuran awal file : 178,13 KB Plaintext : pdfrahasia.pdf Kunci : test Ciphertext : Q4xcLfrCTerLIe.mhi Ukuran akhir file : 178,14 KB

Kesimpulan

Berdasarkan hasil dan pembahasan yang telah dihasilkan pada penelitian ini, dapat disimpulkan:

a. Aplikasi yang dihasilkan dapat digunakan untuk mengamankan *file* dokumen dengan proses enkripsi. Langkah awal dari proses enkripsi *file* dokumen dilakukan dengan memilih *file* dokumen dan menginputkan kunci. Selanjutnya adalah dengan memilih tombol enkrpsi yang terdapat pada aplikasi.
b. Aplikasi akan melakukan proses enkripsi terhadap *file* dokumen menggunakan algoritma beaufort cipher. Selanjutnya hasil enkripsi tersebut dienkripsi kembali menggunakan algoritma hill cipher.
c. Hasil enkripsi menggunakan algoritma hill cipher tersebut merupakan hasil akhir dari proses enkripsi. Hasilnya adalah *file* dokumen tersebut tidak dapat diakses sama sekali menggunakan perangkat lunak apapun.
d. Pada aplikasi juga terdapat menu dekripsi untuk mengembalikan dokumen ke dalam bentuk aslinya.
e. Proses dekripsi dilakukan dengan cara memilih *file* dokumen yang telah dienkripsi dan menginputkan kunci yang sama dengan proses enkripsi. Selanjutnya memilih tombol menu dekripsi.
f. Aplikasi akan memulai proses dekripsi menggunakan algoritma hill cipher. Selanjutnya hasil dekripsi menggunakan algoritma hill cipher didekripsi kembali menggunakan algoritma beaufort cipher.
g. Hasil dekripsi menggunakan algoritma beaufort cipher akan mengembalikan *file* dokumen ke dalam bentuk aslinya sehingga dapat diakses kembali.
h. Pada penelitian ini telah dihasilkan sebuah aplikasi yang dapat digunakan dalam mengamankan *file* dokumen Microsoft Word, Microsoft Excel, dan PDF.
i. Proses pengamanan file dokumen dilakukan menggunakan kombinasi algoritma beaufort cipher dan algoritma hill cipher.

j. Aplikasi pada pelitian ini dikembangkan menggunakan perangkat lunak Android Studio dan hasilnya dapat digunakan pada perangkat *mobile* dengan sistem operasi android.
k. Bahasa pemrograman yang digunakan untuk membangun aplikasi adalah Java dan XML.

Ucapan Terima Kasih

Peneliti mengucapkan banyak terima kasih kepada Universitas Islam Negeri Sumatera Utara yang telah membantu peneliti dalam menyelesaikan pembuatan laporan penelitian ini.

Daftar Pustaka

[1] I. Sari, M. Muttaqin, J. Jamaludin, and J. Simarmata, "Keamanan Data dan Informasi," 2020, Accessed: Apr. 19, 2022. [Online]. Available: https://books.google.com/books?hl=id&lr=&id=WFoMEAAAQBAJ&oi=fnd&pg=PR9&dq=Keamanan+Data+dan+Informasi&ots=T0SVv6tM8U&sig=r3KgDCzQk3FciEm8rpumtdzM7KE

[2] H. Mukhtar, "Kriptografi Untuk Keamanan Data," 2018, Accessed: Apr. 19, 2022. [Online]. Available: https://books.google.com/books?hl=id&lr=&id=bc-HDwAAQBAJ&oi=fnd&pg=PR5&dq=Kriptografi+untuk+Keamanan+Data&ots=zofH3AsTKT&sig=Jx2DIopjgPEAp6rq5vt_HSBwdck.

[3] A. Rachmadsyah, A. Perdana, and A. B. S. T, "Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks Berbasis Mobile Application," vol. 9, no. September, pp. 12–17, 2020.

[4] R. A. Megantara and F. A. Rafrastara, "Super Enkripsi Teks Kriptografi menggunakan Algoritma Hill Cipher dan Transposisi Kolom," *Pros. SENDI_U 2019*, pp. 85–92, 2019.

[5] A. I. Mubarok, A. Hidayat, J. I. Komputer, F. I. Komputer, and U. M. Metro, "Perancangan Aplikasi Pengolahan Data Obat Masuk Dan Keluar Pada Uptd Puskesmas Trimulyo," vol. 01, no. 01, 2021.

[6] A. Khaliq, "APLIKASI MOBILE LEARNING BERBASIS ANDROID UNTUK BELAJAR HURUF HIJAIYAH," *Unnes J. Math.*, vol. 5, no. 2, pp. 108–117, 2021, doi: 10.15294/ujm.v5i2.13119.

[7] D. Taruna, A. Fauzi, and M. C. Aruan, "Aplikasi Pengenalan Dan Pencegahan Bencana Kebakaran Api Yang Disebabkan Oleh Manusia (Human Error) Berbasis Android," *Semna Ristek (Seminar Nas. Ris. dan Inov. Teknol.*, pp. 1–7, 2021.

[8] Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriftografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android.
Jurnal Teknik Informatika Kaputama (JTIK), 3(2), 29-37.

[9] Suhardi. (2016). Aplikasi Kriptografi Data Sederhana Dengan Metode Exclusive-or (Xor). *Jurnal Teknovasi, 03(2), 23-31.*

[10] Verawati, & Liksha, P. D. (2018). Aplikasi Akuntansi Pengolahan Data Jasa Service Pada Pt. Budi Berlian Motor Lampung. *Jurnal Sistem Informasi Akuntansi (JUSITA), 1(1), 1-14.*