CICES (*Cyberpreneurship Innovative and Creative Exact and Social Science*)
DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

Kombinasi *Vigenère* dan *Beaufort Cipher* Konsep Simulasi *Three-pass Protocol* pada Data Penerbangan

Darmeli Nasution[*1], Indri Sulistianingsih[2], Arie Candra Panjaitan[3]
[1, 2]Program Studi Sistem Komputer Universitas Pembangunan Panca Budi Medan Indonesia, [3]Program Studi Sistem Informasi Sekolah Tinggi Manajemen Informatika dan Komputer Institut Teknologi Manajemen Internasional STMIK ITMI Medan Indonesia
E-mail: [*1]**darmelinasution@gmail.com**, [2]indie@pancabudi.ac.id, [3]ariecandra.or@gmail.com

Abstrak

Keamanan komputer sangat penting diterapkan dalam pertukaran data, terutama data penerbangan. Data-data yang dikirim adalah data yang bersifat rahasia. Data ini tidak boleh diketahui oleh orang yang tidak bertanggung jawab. Pencurian data adalah resiko yang dapat terjadi sehingga dapat mengakibatkan kerugian besar. Data-data ini harus dienkripsi sehingga aman pada saat melakukan pengiriman. Pengiriman yang baik tidak perlu melakukan pertukaran kunci sehingga kunci tersebut tidak diberikan kepada penerima yang akan melakukan dekripsi data tersebut. Pengamanan perlu ditingkatkan dengan menggunakan skema Three-pass Protocol dimana skema ini akan mempertahankan agar tidak terjadi pertukaran kunci antara pengirim dan penerima data. Masing-masing pihak akan melakukan proses enkripsi dan dekripsi menggunakan kunci masing-masing. Kunci ini tidak perlu diberikan kepada pihak lain. Konsep Three-pass protocol menggunakan algoritma Vigenère dan Beaufort Cipher. Pengirim akan melakukan proses enkripsi dan dekripsi dengan menggunakan algoritma Vigenère Cipher sementara penerima akan melakukan proses enkripsi dan dekripsi menggunakan algoritma Beaufort Cipher. Data yang terenkripsi secara otomatis akan menjaga keaslian data tersebut pada saat data tersebut kembali didekripsi. Kombinasi kedua algoritma dengan kunci ganda agar hasil enkripsi semakin sulit untuk didekripsi oleh pihak yang tidak berwenang. Hasil dari kombinasi kedua metode ini didapatkan kualitas enkripsi yang lebih baik dibandingkan dengan satu metode Beaufort atau Vigenère saja. Dengan memanfaatkan skema Three-pass Protocol dihasikan data penerbangan akan terjaga kerahasiaannya.

Kata Kunci—*Beaufort; Vigenère; Tiga lintasan; Protokol*

Abstract

Computer security is very important in data exchange, especially flight data. The data sent is confidential data. This data should not be known by irresponsible people. Data theft is a risk that can occur which can result in large losses. This data must be encrypted so that it is safe when sending. Good delivery does not need to exchange keys so that the key is not given to the recipient who will decrypt the data. Security needs to be improved by using the Three-pass Protocol scheme where this scheme will maintain that there is no exchange of keys between the sender and the recipient of the data. Each party will carry out the encryption and decryption process using their respective keys. This key does not need to be given to other parties. The concept of the Three-pass protocol uses the Vigenère and Beaufort Cipher algorithms. The sender will carry out the encryption and decryption process using the Vigenère Cipher algorithm while the recipient will carry out the encryption and decryption process using the Beaufort Cipher algorithm. Encrypted data will automatically maintain the authenticity of the data when the data is decrypted again. The combination of the two algorithms with multiple keys makes the encryption results more difficult to decrypt by unauthorized parties. The result of the combination of these two methods is that the encryption quality is better than the Beaufort or Vigenère methods alone. By utilizing the Three-pass Protocol scheme, flight data will be kept confidential.

Keywords—*Beaufort; Vigenère; Three-pass; Protocol*

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

1. PENDAHULUAN

Penerbangan merupakan kegiatan yang sering dilakukan di dunia. Dalam dunia penerbangan ada data yang penting untuk dikirimkan ke pihak lain. Pengiriman data ini sangat penting dilakukan untuk melakukan pembaharuan data penerbangan itu sendiri. Data-data penting sangat penting dijaga kerahasiaannya agar tidak disalahgunakan oleh orang lain. Terlebih-lebih data penerbangan yang memiliki informasi penting. Pengiriman data yang aman biasanya dilakukan dengan menerapkan teknik kriptografi sehingga pada saat data tersebut terkirim, data ini sudah aman dari pembobolan [1].

Pengiriman data penerbangan membutuhkan kunci pada saat melakukan proses enkripsi agar dapat diacak sebelum dikirimkan [2]. Pihak penerima membutuhkan kunci tersebut dalam usaha mendekripsikan pesan atau data tersebut. Pengirim pada dasarnya harus mengirimkan kunci ke pada penerima agar dapat membuka data tersebut. Tetapi, hal ini dapat menyebabkan kebocoran kunci. Kunci yang dikirimkan akan sangat berpotensi dicuri sehingga dekripsi dapat dilakukan dengan mudah. Dalam memberikan tingkat keamanan yang baik, maka pertukaran kunci tidak boleh dilakukan oleh kedua belah pihak [3].

Dalam memberikan keamanan kunci yang baik, diperlukan suatu teknik untuk menghindari pertukaran kunci. Teknik pada penelitian ini menggunakan skema Three-pass Protocol. Enkripsi dengan skema Three-pass Protocol akan sangat membantu menghindari pertukaran kunci pada saat proses enkripsi dan dekripsi sehingga pengirim data dan penerima data tidak perlu saling mengetahui dan mempertukarkan kunci yang digunakan mereka [4]. Hal ini bertujuan untuk menghindari kebocoran kunci pada saat dikirimkan. Kunci diperlukan untuk melakukan proses dekripsi pada saat data digunakan.

Vigenère Cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenere, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 [5]. Model matematika dari enkripsi pada algoritma vigenere cipher ini adalah seperti berikut:

Model enkripsi Ci = Ek (Mi) = (Mi + Ki) mod 26
Model deskripsi Mi = Dk (Ci) = (Ci -Ki) mod 26
Keterangan:
C: memodelkan ciphertext
M: memodelkan plaintext
K: memodelkan kunci

Beaufort Cipher adalah salah satu varian dari vigenere cipher dimana 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 [6].

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 [6].

Cc = (k-Pc) mod 26
Pc = (k-Cc) mod 26
Keterangan:
C: memodelkan ciphertext
P: memodelkan plaintext
K: memodelkan kunci.

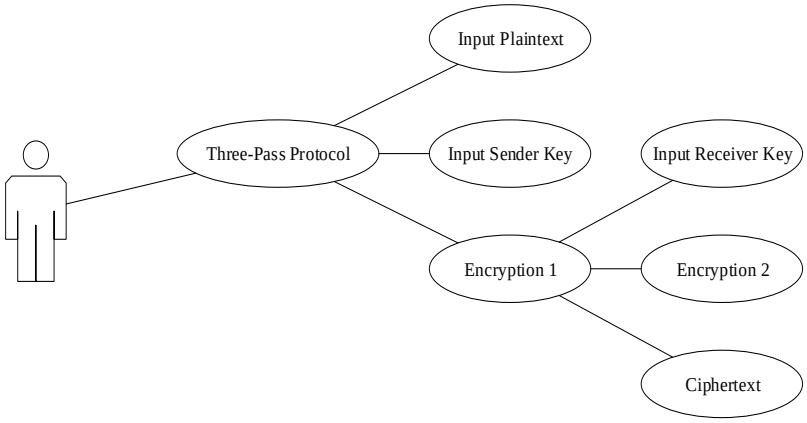
DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

Tujuan penggunaan mengkombinasikan kedua algoritma *Vigenère* dan *Beaufort Cipher* dengan kunci ganda agar hasil enkripsi semakin sulit untuk didekripsi oleh pihak yang tidak berwenang dan dengan memanfaatkan skema *Three-pass Protocol* pada data penerbangan dalam meningkatkan kualitas enkripsi sehingga proses pengiriman data penerbangan akan terjaga kerahasiaannya.

2. METODE PENELITIAN

2.1. Proses Enkripsi

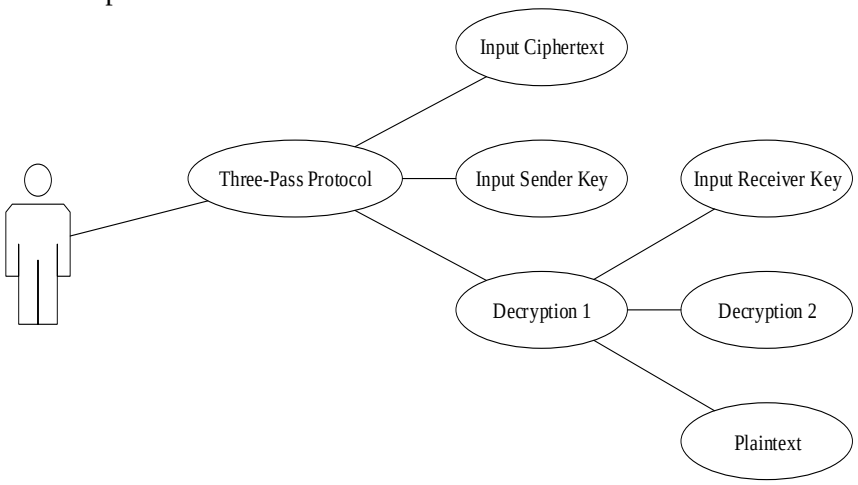
Proses enkripsi pada penelitian ini menggunakan kunci *Vigenère* dan *Beaufort*. Proses enkripsi terjadi dua kali dalam melakukan skema *Three-pass Protocol*. Proses enkripsi akan digunakan oleh pengirim dan penerima dalam melakukan pengiriman data. Proses enkripsi dapat dilihat hirarkinya pada Gambar 1 diagram proses enkripsi.



Gambar 1. Proses Enkripsi

2.2. Proses Dekripsi

Seperti halnya pada proses enkripsi, proses dekripsi pada penelitian ini juga menggunakan kunci *Vigenère* dan *Beaufort*. Proses dekripsi juga terjadi dua kali dalam melakukan skema *Three-pass Protocol*. Proses dekripsi akan digunakan oleh pengirim dan penerima dalam melakukan penerimaan data. Dekripsi harus melakukan proses yang sama dengan proses pada enkripsi. Proses deskripsi dapat dilihat hirarki prosesnya pada Gambar 2 diagram proses dekripsi.



Gambar 2. Proses Dekripsi

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

2.3. Data Penerbangan

Penelitian ini menggunakan sampel data penerbangan yang merupakan jadwal penerbangan dalam beberapa maskapai penerbangan. Pada jadwal tersebut dapat dilihat data-data pesawat dan penumpang. Penelitian ini mencoba menggunakan data berjumlah sepuluh data penerbangan. Data ini akan dienkripsi dengan kedua algoritma sehingga data tersebut menjadi data terenkripsi.

Tabel 1. Data Jadwal Penerbangan

Asal	Maskapai	Kode Penerbangan
UPG Makassar	SJ Sriwijaya Airlines	SJ 0599
SIN Singapore	ID Batik Air	ID 7158
DMK Bangkok Don Mueang	QZ Air Asia Indonesia	QZ 0253
MNL Manila	PR Philipines Airlines	PR 0535
MNL Manila	GA Garuda Indonesia	GA 9987
DPS Bali	JT Lion Airlines	JT 0039
KUL Kuala Lumpur	AK Air Asia	AK 0382
DMK Bangkok Don Mueang	ID Batik Air	ID 7630
ADD Ethiopia	ET Ethiopian Airlines	ET 3600

Tabel 1 menjelaskan beberapa data yang digunakan dalam proses enkripsi dan dekripsi untuk melihat skema *Three-pass protocol*. Ada tiga buah *field* dalam data tersebut yaitu Asal, Maskapai, dan Kode Penerbangan. Data penerbangan ini menggunakan data penerbangan dengan tujuan Soekarno-Hatta International Airport. Setiap data akan dienkripsi menggunakan algoritma *Vigenère* dan *Beaufort* sehingga data tersebut akan terenkripsi dengan baik. Data penerbangan ini akan terenkripsi sebelum dikirim ke penerima sehingga memberikan keamanan dan kenyamanan pada saat data tersebut masih berada pada proses pengiriman.

3. HASIL DAN PEMBAHASAN

Skema Three-pass Protocol merupakan skema pemberian kunci pada proses enkripsi dan dekripsi tanpa harus mempertukarkan kunci kepada pihak pengirim dan penerima. Skema ini digunakan agar kebocoran kunci dapat dihindari. Pertukaran kunci di dunia maya dapat memberikan kesempatan pada hacker dalam usaha membobol kunci tersebut sehingga dapat digunakan dalam membuka pesan terenkripsi.

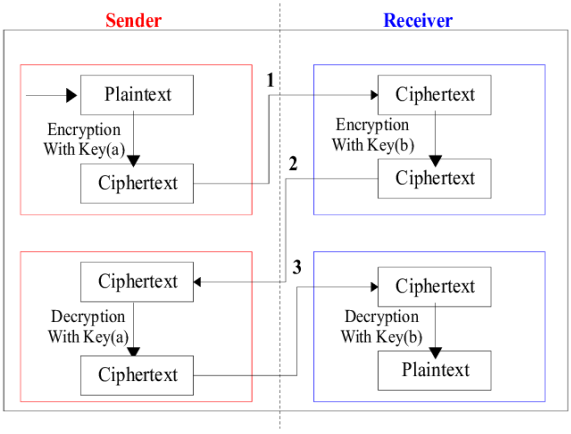
Three-pass Protocol adalah salah satu teknik pada ilmu kriptografi. Pengiriman pesan merupakan hal yang sangat penting dilakukan, tetapi dalam pengiriman pesan dibutuhkan suatu skema kerja yang memungkinkan menjaga kerahasiaan pesan dan kunci saat pengiriman ke pihak penerima. Kerahasiaan kunci dapat dijaga dengan cara tidak bertukar atau mendistribusikan kunci yang digunakan pada dekripsi.

Skema ini adalah *Three-Pass Protocol*. Pengirim dan penerima pesan tidak perlu saling memberitahukan kunci mereka. Kedua pihak akan melakukan tiga tahap proses enkripsi dan

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

akhirnya pesan tersebut akan di dekripsi oleh pihak penerima. Konsep dasar Three-Pass Protocol bahwa kedua pihak memiliki kunci masing-masing yang digunakan pada proses enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci tersebut untuk mengenkripsi pesan dan kemudian untuk mendekripsi pesan pada putaran terakhir.

Gambar 3 adalah skema dari Three-Pass Protocol. Pengirim (*sender*) melakukan enkripsi plaintext dengan menggunakan kuncinya sendiri (Key(a)). Hasil enkripsi adalah merupakan sebuah ciphertext yang sudah tidak dapat dibaca. *Ciphertext* ini akan dikirim ke penerima (*receiver)*. Penerima kemudian melakukan enkripsi kembali dengan menggunakan kunci penerima (Key(b)). Ciphertext kembali dihasilkan. Ciphertext tersebut akan dikirimkan kembali ke pengirim. Setelah menerima ciphertext tersebut, pengirim kembali melakukan dekripsi dengan menggunakan kunci pengirim (Key(a)). Hasil dekripsi masih merupakan sebuah *ciphertext*. *Ciphertext* ini akan dikirim untuk terakhir kalinya ke penerima. Penerima akan melakukan dekripsi dengan menggunakan kunci penerima (Key(b)). Hasil terakhir adalah sebuah plaintext yang sudah dapat dibaca. Dari skema ini terlihat tidak ada pertukaran kunci yang dilakukan antara pengirim dan penerima sehingga kunci tersebut tidak akan dapat dicuri atau dibobol oleh hacker [7].



Gambar 3. Skema Three-pass Protocol
Sumber: [7]

3.1. Beaufort Cipher

Beaufort cipher secara umum merupakan salah satu ilmu kriptografi dalam melakukan penyandian pesan. Algoritma ini merupakan teknik enkripsi substitusi yang akan melakukan pertukaran karakter plaintext berdasarkan pergeseran kunci. Kunci yang digunakan pada algoritma *Beaufort* biasanya merupakan angka pergeseran. Tiap karakter akan menggunakan angka yang berbeda. Panjang kunci tidak selamanya akan sepanjang dengan panjang plaintext. Untuk kunci yang lebih pendek dari plaintext, maka kunci tersebut akan diulang agar memenuhi panjang dari plaintext tersebut.

3.2. Vigenère Cipher

Sandi *Vigenère* adalah algoritma kriptografi yang berfungsi untuk mengubah *plaintext* ke *ciphertext* dengan cara mempertukarkan karakter sesuai dengan kunci yang diberikan pada proses enkripsi dan dekripsi. Sandi *Vigenère* merupakan bentuk sederhana dari pertukaran karakter secara substitusi polialfabetik. Kunci yang digunakan pada algoritma ini akan diulang sehingga memenuhi panjang dari *plaintext* tersebut. Setiap karakter pada plaintext akan dijumlahkan terhadap kunci yang seudah berhasil terbentuk sehingga dapat menghasilkan *ciphertext* berdasarkan karakter baru yang diperoleh. Kelebihan algoritma ini adalah sandi ini tidak begitu

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi terhadap deretan *ciphertext* karena kunci yang digunakan tidak sama untuk setiap karakter plaintext. [8].

Bagian ini akan melakukan pembahasan terhadap proses enkripsi dan dekripsi dengan skema *Three-pass Protocol*. Perhitungan untuk tiap data penerbangan akan dilakukan sehingga membentuk susunan karakter yang baru yang disebut dengan *ciphertext*. Bagian berikut ini adalah contoh perhitungan algoritma *Vigenère* dan *Beaufort* dalam mendapatkan *ciphertext* berdasarkan contoh *plaintext*.

Table 2. Enkripsi Vigenère Cipher

PT	ASC	KEY 1	ASC KEY 1	C1	ASC C1
S	83	M	77	160	†
r	114	a	97	211	”
i	105	k	107	212	‘
w	119	a	97	216	ÿ
i	105	s	115	220	‹
j	106	a	97	203	À
a	97	r	114	211	”
y	121	M	77	198	Δ
a	97	a	97	194	¬
	32	k	107	139	ã
A	65	a	97	162	¢
i	105	s	115	220	‹
r	114	a	97	211	”
l	108	r	114	222	fi
i	105	M	77	182	∂
n	110	a	97	207	œ
e	101	k	107	208	–

Tabel 3. Enkripsi Beaufort Cipher

ASC C1	C1	KEY 2	KEY 1	ASC C2
†	160	3	163	£
”	211	5	216	ÿ
‘	212	7	219	€
ÿ	216	9	225	·
‹	220	3	223	fl
À	203	5	208	–
”	211	7	218	⁄
Δ	198	9	207	œ
¬	194	3	197	≈
ã	139	5	144	ê
¢	162	7	169	©
‹	220	9	229	Â
”	211	3	214	÷
fi	222	5	227	„
∂	182	7	189	Ω
œ	207	9	216	ÿ

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

–	208	3	211	”

Tabel 4. Dekripsi Vigenère Cipher

ASC C2	C2	KEY 1	ASC KEY 1	C3	ASC C3
£	163	M	77	86	V
ÿ	216	a	97	119	w
€	219	k	107	112	p
·	225	a	97	128	Ä
fl	223	s	115	108	l
–	208	a	97	111	o
⁄	218	r	114	104	h
œ	207	M	77	130	Ç
≈	197	a	97	100	d
ê	144	k	107	37	%
©	169	a	97	72	H
Â	229	s	115	114	r
÷	214	a	97	117	u
„	227	r	114	113	q
Ω	189	M	77	112	p
ÿ	216	a	97	119	w
”	211	k	107	104	h

Tabel 5. Dekripsi Beaufort Cipher

ASC C3	C3	KEY 2	KEY 1	PT
V	86	3	83	S
w	119	5	114	r
p	112	7	105	i
Ä	128	9	119	w
l	108	3	105	i
o	111	5	106	j
h	104	7	97	a
Ç	130	9	121	y
d	100	3	97	a
%	37	5	32	

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

H	72	7	65	A
r	114	9	105	i
ASC C3	**C3**	**KEY 2**	**KEY 1**	**PT**
u	117	3	114	r
q	113	5	108	l
p	112	7	105	i
w	119	9	110	n
h	104	3	101	e

Dapat dilihat pada perhitungan tabel sebelumnya, proses enkripsi terjadi dua kali dalam melakukan penyandian data. Sementara, dalam usaha mengembalikan *ciphertext* menjadi *plaintext*, ada dua proses dekripsi dengan algoritma *Vigenère* dan Beaufort yang dilakukan. Tabel 5 adalah hasil plaintext yang diterima oleh penerima. Hasil ini adalah sama dengan *plaintext* sebelumnya yang dijelaskan pada tabel 2. Hasil akhir tidak mengalami perubahan sama sekali. Hal ini berarti proses *Three-Pass Protocol* untuk kedua algoritma telah berjalan dengan benar.

Tabel 6. Data Jadwal Penerbangan Terenkripsi

‘ÙÓÖ	• ÇåÕ×ÖÚ¿	›ÕÖÏ– ¶ÞÄÉâÊÝ ÒÞµØ
¥¶¹ • ÇÝËéÙÚÈ	£° £ØÛáßÐÚÏÅ • © åÖã½ØÓÙ	£°’š«Ÿ²
£¯À £ÏàÑ×ÖèÈÉ	™ª ’ÇæÓá†º¿Ö	™ª’ ¡§›±
”³½ ’ÇàÑáÕäv¨ß Öœ±ì¹ËÜÍ	¡À ‘ÏäŠ·Ùâ·„¹ÖàÓå¹ Ý×Ç	¡À’š¨›¬
• ´¾ • ÇàÓâÇ	˛ ÎÛÖßÖâÄÉãˆ½Í éÀÓÜËí	,’š«™®
• ´¾ • ÇàÓâÇ	—§ — ÇäßÚÇ™ŸÒÔ×êÉ ê½Ë	—§’£¯ž°
”¶Å ’ÇÞÓ	šº œÏáØ– §âÈÐÙÖá×	šº’š¦™²
›»¾ ›ÛÓÖ×†ÅËÑ àÝî	‘± ‘ÏäŠ·Ùâ·	‘±’š©ž«
”³½ ’ÇàÑáÕäv¨ß Öœ±ì¹ËÜÍ	™ª ’ÇæÓá†º¿Ö	™ª’ ¡¬™©
‘ª¶ •ÚÚÓåÖâ·	•º •ÚÚÓåÖâ·Ò • © åÖã½ØÓÙ	•º’ • ¬–©

DOI: 10.33050/cices.v9i2.2699 ISSN: **2356-5209**
pp. 165~173 *Online* ISSN: **2655-3058**

Tabel 6 merupakan hasil enkripsi dari data jadwal penerbangan yang sebelumnya digunakan pada penelitian ini. Tabel 6 merupakan hasil transformasi *plaintext* menjadi ciphertext sesuai dengan data yang ada pada tabel 1 sebelumnya. Kunci yang digunakan pada proses algoritma *Vigenère* adalah XXX, dan kunci algoritma *Beaufort* adalah YYY.

4. KESIMPULAN DAN SARAN

Data penerbangan merupakan data penting yang harus dijaga dalam hal keaslian data. Dalam melindungi data penerbangan, algoritma *Vigenère* dan *Beaufort* sangat baik dikombinasikan dengan menggunakan skema *Three-Pass Protocol* sehingga data tersebut menjadi data terenkripsi. Data ini akan aman apabila dikirimkan ke pihak penerima sehingga tidak akan mengubah susunan data tersebut. Data yang terenkripsi secara otomatis akan menjaga keaslian data tersebut pada saat data tersebut kembali didekripsi. Dengan memanfaatkan skema *Three-pass Protocol*, data penerbangan akan terjaga kerahasiaannya dan Kombinasi kedua algoritma dengan kunci ganda agar hasil enkripsi semakin sulit untuk didekripsi oleh pihak yang tidak berwenang. Hasil dari kombinasi kedua metode ini didapatkan kualitas enkripsi yang lebih baik dibandingkan dengan metode *Beaufort* atau *Vigenère* saja.

DAFTAR PUSTAKA

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 4th ed. New Jersey: Prentice Hall Press, 2013.

[2] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” Int. J. Distrib. Sens. Networks, vol. 10, no. 7, p. 190903, Jul. 2014, doi: 10.1155/2014/190903.

[3] R. Munir, Kriptografi. Bandung: Informatika, 2006.

[4] B. Oktaviana and A. P. U. Siahaan, “Three-Pass Protocol Implementation on Caesar Cipher in Classic Cryptography,” IOSR J. Comput. Eng., vol. 18, no. 4, pp. 26–29, 2016.

[5] Padede, A. M. H., Manurung, H., & Filina, D. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. E-Journal, Vol. 10(No. 2).

[6] Arrijal, I. M. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. E-Journal, Vol. 3(No. 1).

[7] A. Subandi, R. Meiyanti, C. L. M. Sandy, and R. W. Sembiring, “Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification,” Adv. Sci. Technol. Eng. Syst. J., vol. 2, no. 5, pp. 1–5, Jun. 2017, doi: 10.25046/aj020501.

[8] Hidayat, “Algoritma Kriptografi Vigenere Cipher,” 2012. [Online]. Available: https://arfianhidayat.com/algoritma-kriptografi-vigenere-cipher. [Accessed: 04-Nov-2019].