Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

Pengamanan User Account Data Belajar pada E-Task UCIC Menggunakan Algoritma Caesar Cipher Berbasis QR-Code

C Nas
Program Studi Manajemen Informatika, Universitas Catur Insan Cendekia
Jl. Kesambi No. 202, Cirebon, 45133, Indonesia
chairun.nas@cic.ac.id

diterima: 22 Juni 2022
direvisi: 21 Juli 2022
dipublikasi: 1 September 2022

Abstrak

Pandemi Covid-19 yang melanda Indonesia memiliki dampak pada proses pembelajaran mahasiswa Universitas Catur Insan Cendekia, dimana mahasiswa belajar secara daring menggunakan *Learning Management System* yaitu *E-Task UCIC*. Dalam penerapannya, *E-Task UCIC* berisikan materi pembelajaran, absensi kehadiran, tugas, dan ujian mahasiswa yang hanya dapat diakses dengan menggunakan Nomor Induk Mahasiswa (NIM). Penggunaan NIM berdampak tidak terjaganya keamanan data belajar mahasiswa, hal ini dikarenakan NIM bukan merupakan data rahasia, sehingga dapat diketahui oleh banyak orang. Maka untuk menjaga keamanan data belajar mahasiswa diperlukan metode *Kriptografi* pada user akun mahasiswa, dimana hanya mahasiswa yang dapat mengetahui kunci akses ke akun tersebut. Tujuan penelitian ini adalah untuk mengamankan user akun pada data belajar mahasiswa dengan menggunakan metode kriptografi. Dalam penelitian ini, data yang digunakan adalah data *link* akses langsung ke akun mahasiswa, serta kunci akses ke dalam akun. Selanjutnya data tersebut akan dilakukan proses *Kriptografi* dengan menggunakan algoritma *Caesar Cipher*. Hasil dari enkripsi dan dekripsi algoritma dikonversikan kedalam bentuk QR-Code dengan menggunakan *Python*, agar dalam pengaksesan aplikasi lebih cepat dengan proses *scanning*. Maka pengamanan hak akses menggunakan metode *Kriptografi* dengan algoritma *Caesar Cipher* pada data belajar mahasiswa di *E-Task UCIC*, mampu melindungi data belajar mahasiswa untuk tidak dapat dimasuki tanpa menggunakan kunci akses dan QR-Code dari mahasiswa tersebut.
Kata kunci: Keamanan; Data; Kriptografi; Caesar Cipher; QR-Code

Abstract

The Covid-19 pandemic that hit Indonesia had an impact on the learning process of Catur Insan Cendekia University students, where students studied online using the Learning Management System, namely the UCIC E-Task. In its application, the UCIC E-Task contains learning materials, attendance, assignments, and student exams that can only be accessed using the Student Identification Number (NIM). The use of the NIM has an impact on the security of student learning data, this is because the NIM is not confidential data, so it can be known by many people. So to maintain the security of student learning data, a Cryptographic method is needed on the student account user, where only students can find out the access key to the account. The purpose of this study is to secure user accounts on student learning data using cryptographic methods. In this study, the data used are direct access data links to student accounts, as well as access keys to accounts. Furthermore, the data will be cryptographic process using the Caesar Cipher algorithm. The results of the encryption and decryption algorithm are converted into QR-Code form using Python, so that the application access is faster with the scanning process. So securing access rights

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

using the Cryptography method with the Caesar Cipher algorithm on student learning data at UCIC E-Task, is able to protect student learning data from being entered without using the access key and QR-Code from the student..
Keywords: *Security; Data; Cryptography; Caesar Cipher; QR-Code*

1. Pendahuluan

Awal kemunculan virus Covid-19 di Indonesia hingga sampai saat ini telah memberikan dampak yang sangat besar diberbagai sektor dalam kehidupan masyarakat Indonesia, seperti sektor ekonomi, pendidikan, transportasi dan lainnya. Pemerintah mengeluarkan aturan-aturan untuk membatasi kegiatan masyarakat diluar rumah agar dapat menekan penyebaran virus Covid-19, sehingga semua kegiatan masyarakat dilakukan dirumah masing-masing dan dilakukan secara daring. Aturan ini juga berlaku di sektor pendidikan, dimana proses belajar mengajar siswa dan guru dilakukan secara daring dengan menggunakan aplikasi berbasis online seperti *Google Meet*, *Zoom*, *Microsoft Team* dan *Learning Management System* (LMS) lainnya, sehingga hampir semua institusi pendidikan berusaha mengembangkan LMS sendiri untuk memenuhi kebutuhan proses belajar mengajar siswa. Namun dengan hadirnya LMS memiliki dampak positif terhadap kegiatan belajar mengajar, dimana pembelajaran lebih praktis, informasi lebih cepat dan menjangkau ruang lingkup yang luas serta memberikan pengalaman baru dalam kegiatan belajar mengajar [1].

Sebagai Institusi Pendidikan Tinggi, Universitas Catur Insan Cendekia dimasa pandemi Covid-19 mengembangkan LMS *E-Task UCIC* untuk proses belajar mengajar mahasiswa dan dosen secara daring. Penggunaan *E-Task UCIC* ini dapat dilakukan oleh dosen dan mahasiswa untuk mengupload dan memperoleh materi pembelajaran, absensi kehadiran setiap pertemuan, tugas matakuliah serta pengerjaan Quis dan Ujian Tengah Semester maupun Ujian Akhir Semester. Dalam pelaksanaannya, *E-Task UCIC* dapat dibuka dengan mengakses link website dan untuk masuk ke akun mahasiswa harus menggunakan Nomor Induk Mahasiswa (NIM) yang dimiliki oleh mahasiswa tersebut. Penggunaan NIM dalam mengakses akun mahasiswa, memiliki dampak tidak terjaganya data belajar mahasiswa dengan baik [2]. Hal ini dikarenakan NIM mahasiswa bukanlah data rahasia, sehingga NIM mahasiswa dapat diketahui oleh banyak orang dan mengakibatkan adanya orang lain yang dapat mengakses ke akun data belajar mahasiswa pada *E-Task UCIC*. Maka untuk mengatasi permasalahan tersebut, perlu adanya pengamanan hak akses mahasiswa pada *E-Task UCIC* melalui proses metode *kriptografi*.

Metode kriptografi bertujuan untuk menyembunyikan atau merahasiakan suatu keaslian data dengan melakukan proses enkripsi dan dekripsi sehingga tidak dapat diketahui oleh orang yang tidak memiliki hak terhadap data tersebut [3]. Didalm proses metode kriptografi, terdapat algoritma-algoritma untuk melakukan proses enkripsi dan dekripsi, salah satunya adalah algoritma *Caesar Cipher*. Algoritma *Caesar Cipher* merupakan penyandian substitusi pada sebuah huruf yang akan di enkripsi, ditukarkan dengan huruf lain yang memiliki perbedaan tempat tertentu didalam *alphabet* [4]. Hasil enkripsi menggunakan algoritma *Caesar Cipher* selanjutnya dapat di *generate* kedalam bentuk QR-Code. QR-Code merupakan teknik mengubah data tertulis menjadi kode-kode 2 dimensi yang ditampilkan kedalam suatu gambar yang lebih ringkas [5]. QR-Code menyimpan data-data kedalam bentuk kode yang lebih ringkas, sehingga berbentuk sederhana namun keamanan data dapat terjaga dengan baik.

Dalam penelitian sebelumnya, penggunaan algoritma *Caesar Cipher* dalam proses *kriptografi* digunakan untuk pengamanan data Kartu Ujian siswa melalui scan QR-Code. Pada penelitian ini, QR-Code diperoleh melalui hasil enkripsi dari Nomor Ujian siswa dan

di *generate* kedalam bentuk QR-Code. Selanjutnya, untuk masuk kedalam sistem, QR-Code tersebut akan di scan dan sistem akan mendekripsikan QR-Code menjadi Nomor Ujian siswa dan akan mengeluarkan kartu Ujian Siswa. Hasil dari penelitian ini, siswa dapat memperoleh kartu ujian melalui akses aplikasi dengan QR-Code siswa masing-masing, sehingga orang lain tidak dapat mengakses ke akun siswa [6].

Algoritma *Caesar Cipher* juga dilakukan pada penelitian untuk pengamanan data pesan email di Exo Digital Agency. Pada penelitian ini, sebuah pesan yang akan dikirim terlebih dahulu di enkripsi dengan algoritma *Caesar Cipher* yang sudah diimplementasikan kedalam Aplikasi email. Selanjutnya, dengan data kunci yang dimiliki oleh penerima pesan, maka pesan tersebut di dekripsi agar sipenerima dapat membuka dan membaca pesan tersebut. Hasil dari penelitian ini adalah pesan yang dikirim tidak dapat dicuri oleh pihak lain, serta waktu proses enkripsi dan dekripsi yang cepat dengan waktu 0,004 *second* [7].

Berdasarkan penelitian terdahulu, maka terdapat perbedaan dengan penelitian yang telah dilakukan yaitu pada proses pengamanan user akun. Pengamanan user akun dilakukan melalui 2 tahapan, yaitu tahapan kriptografi untuk memperoleh enkripsi dan tahapan *generate* hasil enkripsi ke bentuk QR-Code agar pihak lain tidak mengetahui hasil enkripsi dari data asli, sehingga terdapat 2 lapisan pengamanan data. Dari penjelasan tersebut, pengamanan user akun pada data belajar mahasiswa menggunakan metode Kriptografi dengan algoritma *Caesar Cipher* yang di *generate* kedalam bentuk QR-Code dapat digunakan untuk menjaga data user akun, dengan hasil akhir adalah hanya mahasiswa yang memiliki kunci akses serta QR-Code tersebut yang dapat mengakses data belajarnya di aplikasi E-TASK UCIC.

2. Kajian Pustaka

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang berarti tersembunyi. Kriptografi dapat diartikan sebagai disiplin ilmu yang mempelajari teknik penyandian pesan dengan aspek keamanan data seperti [8]:

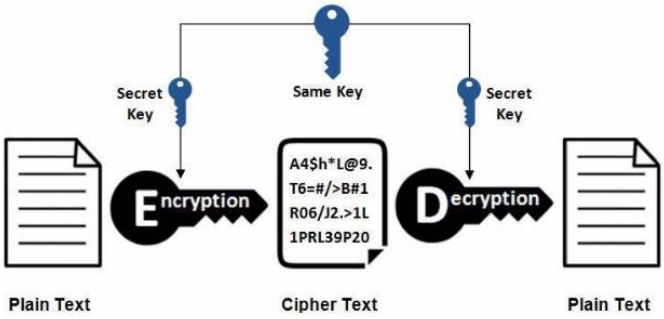
a. Kerahasiaan (*confidentiality*)
   Merupakan aspek untuk menjaga informasi agar tidak dapat dibaca oleh pihak-pihak yang tidak memiliki hak akses.
b. Keaslian Data (*data integrity*)
   Merupakan aspek untuk menjamin keaslian dari suatu informasi dan tidak dimanipulasi oleh pihak lain selama pengiriman informasi.
c. Autentifikasi Data (*authentication*)
   Merupakan aspek yang berhubungan dengan identifikasi kebenaran dari informasi yang dikirim oleh pengirim dan penerima informasi.
d. *Non-repudiation*
   Merupakan aspek untuk menjaga entitas dari pengirim dan penerima tidak menyangkal informasi yang dikirim maupun diterima.

Kriptografi bertujuan untuk mengurangi resiko ancaman keamanan dengan melakukan proses enkripsi dan dekripsi pada data dan informasi [9]. Enkripsi merupakan proses dimana suatu informasi dan data ditransmisikan kedalam bentuk penyandian sehinggan berbeda dengan informasi dan data awalnya, sedangkan dekripsi merupakan proses pembalikan informasi dan data yang telah disandikan kedalam bentuk inofrmasi dan data awal [10]. Dalam Kriptografi terdapat 2 teknik penyandian yaitu simetris dan asimetris, dimana simetris menggunakan kunci yang sama untuk melakukan proses enkripsi dan

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

dekripsi, sedangkan asimetris menggunakan kunci publik (umum) pada proses enkripsi dan kunci privat untuk proses dekripsi [11].

Dalam penelitian teknik penyandian yang akan dilakukan adalah teknik simetris, dimana untuk proses enkripsi dan dekripsi menggunakan kunci privat yang sama. Adapun bentuk umum dari teknik simetris dapat dilihat pada Gambar 1 [4].



Gambar 1. Bentuk UmumTeknik Simetris

Pada Gambar 1 dapat dijelaskan bahwa teknik simetris hanya menggunakan 1 kunci rahasia dalam mengacak dan menguraikan informasi. Kunci rahasi tersebut dapat berupa angka, kata atau serangkaian huruf acak. Oleh karena itu, hanya pengirim dan penerima informasi yang dapat mengetahui kunci rahasia dalam melakukan proses enkripsi dan dekripsi informasi.

Berdasarkan penjelasan sebelumnya, maka teknik simetri dalam penyandian informasi cocok untuk mengamankan suatu informas. Salah satu algoritma yang umum digunakan pada teknik simetris ini adalah algoritma *Caesar Cipher*.

2.2 Algoritma Caesar Cipher

Algoritma *Caesar Cipher* merupakan jenis penyandian substitusi dimana setiap huruf awal di geser sesuai susunannya dengan kunci berdasarkan abjad pada ASCII (*American Standard Code for Information Interchange*) [12]. Dalam penggunan algoritma *Caesar Cipher* terdapat 2 langkah sederhana, yaitu [13]:

a. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk *ciphertext* ke *plaintext*.
b. Menukarkan karakter pada *plaintext* menjadi *cipherteks* dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Maka berdasarkan langkah-langkah algoritma *Caesar Cipher* tersebut, maka terdapat rumus untuk memproses enkripsi dan dekripsi dari *plaintext* sebagai berikut:

Enkripsi

$$E(x) = x + K \ mod \ 26 \quad (1)$$

Dekripsi

$$D(x) = x - K \ mod \ 26 \quad (2)$$

Dari rumus tersebut, nilai *K* merupakan nilai kunci yang digunakan untuk menggeser setiap karakter *x*. Algoritma *Caesar Cipher* dalam proses enkripsi suatu *plaintext* dapat dimodifikasi dengan tujuan untuk menyederhanakan hasil *ciphertext* agar tidak menggunakan simbol-simbol yang tidak terdapat pada keyboard. Modifikasi yang dilakukan adalah dengan mengubah nilai modulus 26 menjadi modulus 95, hal ini dikarenakan plaintext akan dirubah kedalam 95 karakter yang telah ditentukan, yaitu

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

karakter dari nomor 32 sampai dengan karakter nomor 126 pada ASCII atau dapat disebut dengan *ASCII Printable Characters* yang dapat dilihat pada Gambar 1 [14].

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Gambar 1. *ASCII Printable Character*

Dengan modifikasi yang diterapkan, maka rumus untuk proses enkripsi dan dekripsi dapat dilihat sebagai berikut [14]:

Enkripsi

$$E(x) = \big((x - spasi + K) mod\ 95\big) + spasi \quad (3)$$

Dekripsi

$$D(x) = \big((95 + x - spasi - K) mod\ 95\big) + spasi \quad (4)$$

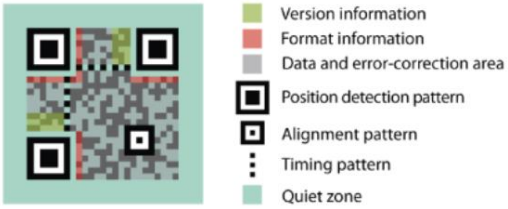
Dimana *spasi* dalam rumus 3 dan 4 merupakan nomor karakter dari spasi pada *ASCII Printable Character* yang bertujuan untuk membatasi hasil *chipertext* dan *plaintext* agar dimulai pada nomor 32 pada ASCII.

2.3 Quick Response (QR) Code

Quick Response (QR) *Code* atau dapat disebut dengan kode respon cepat adalah suatu jenis *image* dua dimensi yang berisikan data berupa teks dengan tujuan untuk menyampaikan informasi dengan cepat dan mendapatkan respon yang cepat dengan cara pemindaian [15]. QR-Code mampu menyimpan semua jenis data, seperti data angka/numerik, *alphanumeric*, biner, kanji/kana. QR-Code mampu menampung data secara horizontal dan vertikal, selain dari itu QR-Code juga tahan terhadap kerusakan, maka walaupun sebagian simbol QR-Code rusak, data tetap dapat disimpan dan dibaca [5].

Setiap simbol QR-Code disusun dalam bentuk persegi dan terdiri dari *function patterns* yang meliputi *finder patterns*, *separators*, *timing patterns* dan *alignment patterns*, serta *encoding region* yang berisikan data mengenai informasi versi, format informasi dan data dan koreksi kesalahan [16]. Adapun struktur QR Code dapat dilihat pada Gambar 2 [16].

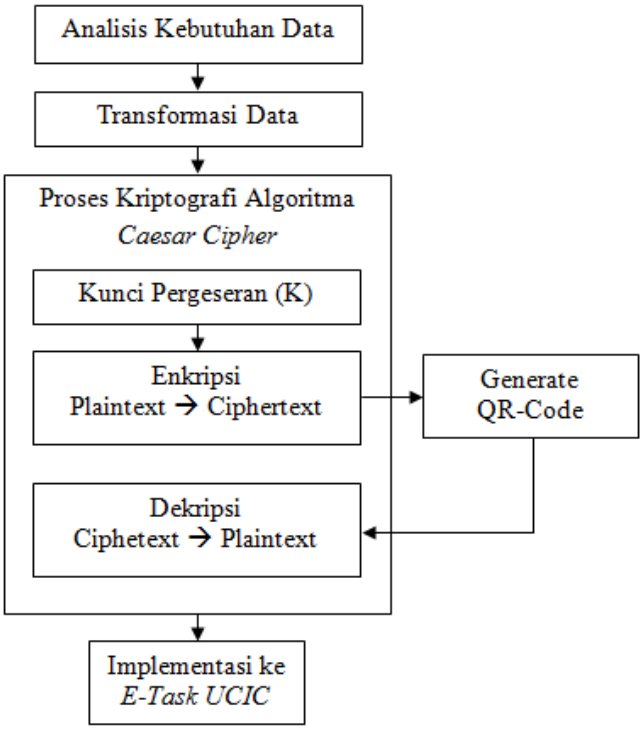
Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2



Gambar 2. Struktur QR-Code

3. Metode Penelitian

Pada penelitian ini, dijelaskan tahapan-tahapan dalam pengamanan data belajar mahasiswa dalam aplikasi *E-Task UCIC* melalui proses kriptografi menggunakan algoritma *Caesar Cipher* pada data user akses mahasiswa, dan digenerate kedalam bentuk QR-Code agar mempercepat akses aplikasi. Adapun tahapan yang dilakukan dapat dilihat pada Gambar 3.



Gambar 3. Tahapan Proses Penelitian

3.1 Analisis Kebutuhan Data

Kebutuhan data dalam penelitian ini adalah data berupa *link* akses langsung ke akun mahasiswa, hal ini bertujuan agar mahasiswa tidak perlu lagi memasukkan *username* dan *password*, melainkan hanya tinggal scan QR-Code. Data *link* akses ini disebut sebagai *plaintext*, adapun *plaintext* yang digunakan sebagai data adalah "**https://etask.cic.ac.id /drive/folders/1VoRAFRXyw4pqVHS9Lgsc5**". Setiap mahasiswa memiliki link akses yang berbeda, sehingga hasil generate QR-Code dan kunci akses setiap mahasiwa juga berbeda. QR-Code dan kunci akses yang digunakan oleh mahasiswa setiap kali menggunakan aplikasi E-TASK UCIC adalah QR-Code dan kunci akses yang sama. Selain dari *plaintext*, data lain yang dibutuhkan adalah *ASCII Printable Character* sebagai nilai transformasi *plaintext*.

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

3.2 Transformasi Data

Transformasi Data adalah perubahan data dengan mengubah nilai atribut awalnya menjadi nilai atribut yang sesuai dengan kebutuhan data dalam pengolahannya [17]. Berdasarkan *plaintext* yang sudah dimiliki, maka *plaintext* di transformasi kedalam nilai karakter yang ada pada *ASCII Printable Character* dengan hasil seperti Tabel 1.

Tabel 1. Transformasi *Plaintext* Ke Nilai Karakter *ASCII*

Plaintext	Nilai *ASCII*	Plaintext	Nilai *ASCII*	Plaintext	Nilai *ASCII*	Plaintext	Nilai *ASCII*
h	104	i	105	f	102	X	88
t	116	c	99	o	111	y	89
t	116	.	46	l	108	w	119
p	112	a	97	d	100	4	52
s	115	c	99	e	101	p	112
:	58	.	46	r	114	q	113
/	47	i	105	s	115	V	86
/	47	d	100	/	47	H	72
e	101	/	47	1	49	S	83
t	116	d	100	V	86	9	57
a	97	r	114	o	111	L	76
s	115	i	105	R	82	g	103
k	107	v	118	A	65	s	115
.	46	e	101	F	70	c	99
c	99	/	47	R	82	5	53

Berdasarkan nilai *ASCII* yang diperoleh dari *plaintext*, maka nilai tersebut akan digunakan didalam proses enkripsi pada algoritma *Caesar Cipher*.

3.3 Proses Algoritma Caesar Cipher & Generate QR-Code

Hasil transformasi data yang telah didapatkan, selanjutnya digunakan untuk proses pada Algoritma *Caesar Cipher*. Tahapan dalam Algoritma *Caesar Cipher* dikelompokkan menjadi 2, yaitu proses enkripsi dan dekripsi, adapun tahapan tesebut dapat dijelaskan sebagai berikut:

1) Menentukan kunci pergeseran, adapun kunci pergeseran yang ditentukan sebagai contoh kasus yaitu 18.
2) Selanjutnya melakukan proses enkripsi dari nilai karakter *ASCII* setiap *plaintext*. Dari enkripsi tersebut, dihasilkan *chipertext* seperti pada Tabel 2.
3) Hasil dari *chipertext* selanjutnya di *generate* kedalam bentuk QR-Code dengan menggunakan *python* seperti pada Gambar 4.
4) Untuk proses dekripsi, hasil QR-Code akan kembali di *generate* kedalam bentuk *chipertext* dan merubah kembali kedalam bentuk plaintext menggunakan kunci pergeseran yang sama. Proses dekripsi dapat dilihat pada Tabel 3.

3.4 Implementasi

Implementasi dilakukan dengan menerapkan algoritma *Caesar Cipher* pada aplikasi E-Task UCIC, terutama pada proses enkripsi dan dekripsi data user akun mahasiswa, selain dari itu ada form *scanning* QR-Code sebagai pengganti form login. Maka dari itu data belajar mahasiswa pada aplikasi *E-Task UCIC* hanya dapat diakses oleh mahasiswa yang memiliki QR-Code dan kunci akses saja, hal ini akan meminimalkan tingkat pencurian data belajar mahasiswa oleh pihak lain.

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

4. Hasil dan Pembahasan

Berdasarkan metodologi penelitian, maka dapat dijelaskan tahapan proses algoritma *Caesar Cipher* untuk pengamanan user akun data belajar mahasiswa pada aplikasi *E-Task UCIC*. Adapun tahapan proses yang akan dilakukan adalah sebagai berikut.

Langkah pertama adalah melakukan proses enkripsi dari *plaintext* yang sudah di transformasi ke nilai karakter *ASCII Printable Character* pada Tabel 1. Enkripsi dilakukan untuk mendapatkan nilai *ciphertext* dengan menggunakan rumus modifikasi pada enkripsi dan menggunakan kunci pergeseran yang telah ditentukan. Adapun proses enkripsi dapat dilihat sebagai berikut.

$$H(104) = \left((104 - 32 + 18) mod\ 95\right) + 32 \quad = 122$$
$$T(116) = \left((116 - 32 + 18) mod\ 95\right) + 32 \quad = 39$$
$$T(116) = \left((116 - 32 + 18) mod\ 95\right) + 32 \quad = 39$$
$$P(112) = \left((112 - 32 + 18) mod\ 95\right) + 32 \quad = 35$$
$$S(115) = \left((115 - 32 + 18) mod\ 95\right) + 32 \quad = 38$$
....
....
$$5(53) = \left((53 - 32 + 18) mod\ 95\right) + 32 \quad = 71$$

Setelah diperoleh nilai *ciphertext* untuk semua *plaintext*, selanjutnya dilakukan transformasi kedalam bentuk karakter sesuai dengan *ASCII Printable Character*, seperti pada Tabel 2.

Tabel 2. Transformasi Nilai *Ciphertext* Dari Hasil Enkripsi ke Karakter *ASCII*

Plaintext Awal	Hasil Enkripsi	Karakter *Ciphertext*
h	122	z
t	39	'
t	39	'
p	35	#
s	38	&
:	76	L
/	65	A
/	65	A
e	119	w
t	39	'
a	115	s
s	38	&
k	125	}
.	64	@
c	117	u
i	123	{
c	117	u
.	64	@
a	115	s
c	117	u
.	64	@
i	123	{
d	118	v

Plaintext Awal	Nilai Enkripsi	Karakter *Ciphertext*
f	120	x
o	34	"
l	126	~
d	118	v
e	119	w
r	37	%
s	38	&
/	65	A
1	67	C
V	104	h
o	34	"
R	100	d
A	83	S
F	88	X
R	100	d
X	106	j
y	107	k
w	42	*
4	70	F
p	35	#
q	36	$
V	104	h
H	90	Z

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

/	65	A	S	101	e
d	118	v	9	75	K
r	37	%	L	94	^
i	123	{	g	121	y
v	41	)	s	38	&
e	119	w	c	117	u
/	65	A	5	71	G

Berdasarkan Tabel 2, maka diperoleh hasil *ciphertext* dari *plaintext* awal yaitu, "**z''#&LAAw's&}@u{u@su@{vAv%{)wAx"~vw%&Ach"dSXdjk*F#$hZeK^y&uG**" . Dari hasil chipertext tersebut, maka akan dilakukan proses *generate* QR-Code.

Langkah kedua setelah diperolehnya hasil *ciphertext* adalah melakukan proses *generate* kedalam bentuk QR-Code. Proses *generate* dilakukan dengan menggunakan python. Adapun koding *python* untuk melakukan *generate ciphertext* dapat dilihat sebagai berikut.

```
import qrcode
qr = qrcode.QRCode(
    version=1,
    error_correction=qrcode.constants.ERROR_CORRECT_L,
    box_size=10,
    border=4,)

qr.add_data("z"#&LAAw's&}@u{u@su@{vAv%{)wAx~vw%&AchdSXdjk*F#$hZeK^y&uG")
qr.make(fit=True)

img = qr.make_image(fill_color="black", back_color="white")
img.save("QRCode_Mahasiswa.png")
```

Hasil enkripsi *ciphertext* yang telah diperoleh dimasukkan kedalam koding *python* sebelumnya. Dari hasil pemproses koding *python*, maka dapat diperoleh hasil generate QR-Code seperti pada Gambar 4 berikut:

Gambar 4. Hasil *Generate* QR-Code

Langkah selanjutnya adalah proses dekripsi untuk mengubah *ciphertext* menjadi *plaintext* dengan menggunakan kunci pergeseran yang sama. Dalam proses ini, digunakan rumus modifikasi dari dekripsi untuk mengubah ciphertext menjadi plaintext awal. Adapun proses dekripsi dapat dilihat sebagai berikut.

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

$$z(122) = \big((95 + 112 - 32 - 18) mod\ 95\big) + 32 = 104$$
$$'(39) = \big((95 + 39 - 32 - 18) mod\ 95\big) + 32 = 116$$
$$'(39) = \big((95 + 39 - 32 - 18) mod\ 95\big) + 32 = 116$$
$$\#(39) = \big((95 + 35 - 32 - 18) mod\ 95\big) + 32 = 112$$
$$\&(38) = \big((95 + 38 - 32 - 18) mod\ 95\big) + 32 = 115$$

.....

.....

$$G(71) = \big((95 + 71 - 32 - 18) mod\ 95\big) + 32 = 53$$

Setelah diperoleh nilai karakter *plaintext* untuk semua *ciphertext*, selanjutnya dilakukan transformasi kedalam bentuk karakter sesuai dengan *ASCII Printable Character*, seperti pada Tabel 3.

Tabel 3. Transformasi Nilai *Plaintext* Dari Hasil Dekripsi ke Karakter *ASCII*

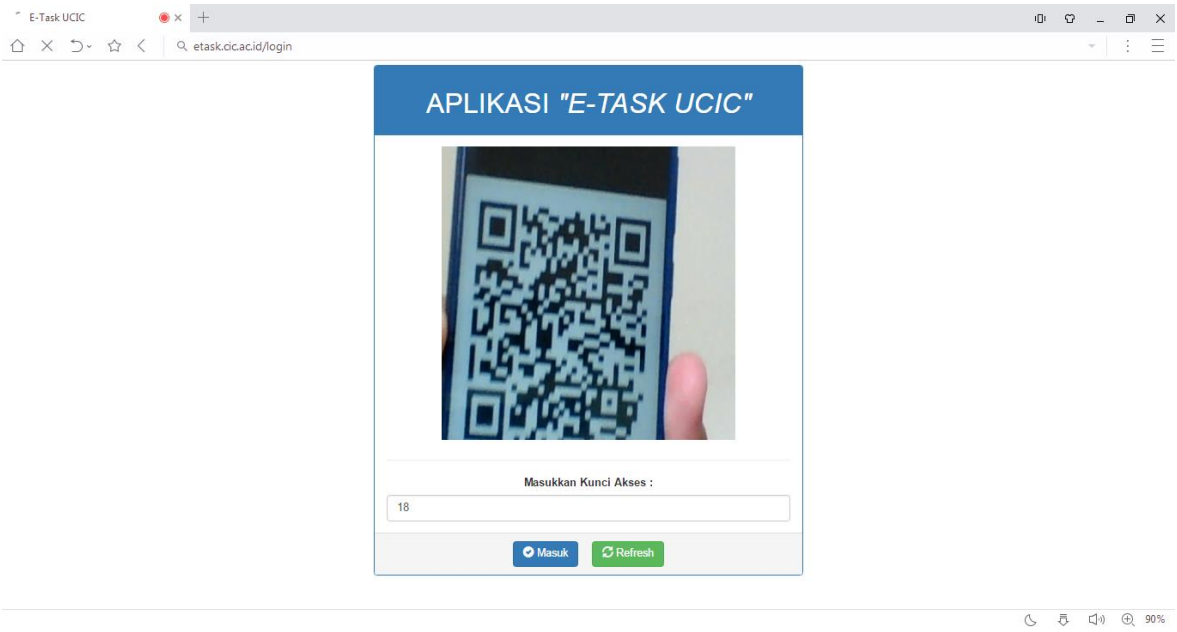
Ciphertext	Hasil Dekripsi	Karakter *Plaintext*	*Ciphertext*	Hasil Dekripsi	Karakter *Plaintext*
z	104	h	x	102	f
'	116	t	"	111	o
'	116	t	~	108	l
#	112	p	v	100	d
&	115	s	w	101	e
L	58	:	%	114	r
A	47	/	&	115	s
A	47	/	A	47	/
w	101	e	C	49	1
'	116	t	h	86	V
s	97	a	"	111	o
&	115	s	d	82	R
}	107	k	S	65	A
@	46	.	X	70	F
u	99	c	d	82	R
{	105	i	j	88	X
u	99	c	k	89	y
@	46	.	*	119	w
s	97	a	F	52	4
u	99	c	#	112	p
@	46	.	$	113	q
{	105	i	h	86	V
v	100	d	Z	72	H
A	47	/	e	83	S
v	100	d	K	57	9
%	114	r	^	76	L
{	105	i	y	103	g
)	118	v	&	115	s
w	101	e	u	99	c
A	47	/	G	53	5

Berdasarkan Tabel 3, maka diperoleh hasil *plaintext* dari *ciphertext* yaitu, "**https://etask.cic.ac.id/drive/folders/1VoRAFRXyw4pqVHS9Lgsc5**". Maka dengan

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN2655-6839
DOI 10.34010/jati.v12i2

menggunakan algoritma *Caesar Cipher* dapat mengamankan user akun data belajar mahasiswa menggunakan QR-Code dan kunci akses yang hanya di ketahui oleh mahasiswa.

Berdasarkan proses kriptografi dengan menggunakan algoritma *Caesar Cipher*, maka proses-proses tersebut dapat diimplementasikan ke dalam aplikasi *E-Task UCIC*. Implementasi dilakukan pada bagian form *Log In* di aplikasi, dimana sebelumnya untuk proses masuk ke dalam sistem *E-Task UCIC* menggunakan *username* dan *password*, setelah dilakukan implementasi algoritma *Caesar Cipher* berbasis QR Code, maka bagian memasukkan *username* dan *password* diganti menjadi proses *scan* QR-Code dan memasukkan kunci akses. Adapun hasil implementasi algoritma *Caesar Cipher* untuk bagian *Log In* dapat dilihat pada Gambar 5.



Gambar 5. Bagian *Log In* Aplikasi E-Task UCIC

Setelah melakukan *scanning* dan memasukkan kunci akses, selanjutnya akan diarahkan ke halaman dashboard data belajar mahasiswa sebagai wadah bagi mahasiswa mengelola data belajar seperti modul pembelajaran, tugas, absensi perkuliahan dan lain-lainnya.

5. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, proses enkripsi data pada algoritma *Caesar Cipher* mampu menghasilkan *ciphertext* yang unik dengan menggunakan kunci pergeseran yang telah ditentukan oleh setiap mahasiswa. Sehingga tanpa mengetahui kunci pergeseran yang tepat, maka data yang telah di enkripsi akan susah untuk dipecahkan. Selain dari itu, melakukan *generate* terhadap *ciphertext* yang telah dihasilkan kedalam bentuk QR-Code mampu meningkatkan keamanan dari data akun akses yang telah di enkripsikan, hal ini dikarenakan data diganti kedalam bentuk *image* 2 dimensi yang sulit untuk dipahami. Selain dari itu penggunaan QR-Code memberikan kemudahan dan kecepatan bagi mahasiswa untuk mengakses data belajar, tanpa harus memasukkan *username* dan *password* yang sulit untuk diingat. Sehingga dapat disimpulkan bahwa penggunaan algoritma *Caesar Cipher* telah dapat mengamankan data belajar mahasiswa pada aplikasi *E-Task UCIC* melalui proses enkripsi dan dekripsi pada user akun mahasiswa yang telah di *generate* kedalam bentuk QR-Code. Untuk penelitian lebih lanjut, proses

enkripsi dan dekripsi data dapat dikombinasikan dengan menggunakan algoritma-algoritma kriptografi lainnya, sehingga enkripsi data yang dihasilkan lebih unik dan sulit untuk dipecahkan.

Daftar Pustaka

[1] N. N. S. Adi, D. N. Oka dan N. M. S. Wati, "Dampak Positif dan Negatif Pembelajaran Jarak Jauh di Masa Pandemi Covid-19," Jurnal Ilmiah Pendidikan Dan Pembelajaran, vol. 5, no. 1, pp. 43–48, 2021, E-ISSN : 2615-6091. Tersedia: https://ejournal.undiksha.ac.id/index.php/JIPP/article/view/32803. [Diakses: 11-Juni-2022]

[2] A. Saputra, Nelmiawati dan M. A. R. Sitorus, "Penilaian Ancaman Pada Website Transkip Aktivitas Kemahasiswaan Politeknik Negeri Batam Menggunakan Metode DREAD," Jurnal Integrasi, vol. 9, no. 1, pp. 53–66, 2017, E-ISSN : 2548-9828. Tersedia: https://jurnal.polibatam.ac.id/index.php/JI/article/view/281. [Diakses: 11-Juni-2022]

[3] M. I. Zulfikar, G. Abdillah dan A. Komarudin, "Kriptografi Untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)," Seminar Nasional Aplikasi Teknologi Informasi, Agustus 2019. Tersedia: https://journal.uii.ac.id/Snati/article/download/13420/9500/0. [Diakses: 11-Juni-2022]

[4] Hermansa, R. Umar dan A. Yudhana, "Pengamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra," Jurnal Sains Komputer & Informatika, vol. 4, no. 1, pp. 157-169, E-ISSN : 2549-7200. Tersedia: http://tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/195/177. [Diakses: 11-Juni-2022]

[5] N. A. Musthofa, S. Mutrofin dan M. A. Murthado, "Implementasi Quick Response (QR) Code Pada Aplikasi Validasi Dokumen Menggunakan Perancangan Unified Modelling Language (UML)," Jurnal Antivirus, vol. 10, no. 1, pp. 42-50, 2016, E-ISSN : 2527-337X. Tersedia: https://ejournal.unisbablitar.ac.id/index.php/antivirus/article/download/87/83/. [Diakses: 13-Juni-2022]

[6] Andriyanto, "Implementasi Algoritma Caesar Cipher Untuk Keamanan Data Pada Kartu Ujian," Jurnal Buffer Informatika, vol. 5, no. 1, pp. 1-7, 2019, E-ISSN : 2614-5413. Tersedia: https://journal.uniku.ac.id/index.php/buffer/article/view/1953. [Diakses: 13-Juni-2022]

[7] R. A. Hamdan dan Painem, "Implementasi Kriptografi Menggunakan Metode Caesar Cipher Dan Vigenere Cipher Untuk Mengamankan Email Pada Exo Digital Agency ," Jurnal SKANIKA, vol. 1, no. 1, pp. 243–250, 2018, E-ISSN : 2721-4788. Tersedia: https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/188. [Diakses: 13-Juni-2022]

[8] C. A. Sari dan W. S. Sari, "Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna," Jurnal Masyarakat Informatika, vol. 13, no. 1, pp. 45–58, 2022, E-ISSN : 2777-0648. Tersedia: https://ejournal.undip.ac.id/index.php/jmasif/article/view/43314/21561. [Diakses: 16-Juni-2022]

[9] E. E. Awal, E. H. Nurkifli dan T. N. Padilah, "Analisis Perbandingan Hasil Enkripsi Dan Dekripsi Algoritma Kriptografi Rijndael Dan Twofish Untuk Penyandian Data," Jurnal Mahasiswa Ilmu Komputer, vol. 3, no. 1, pp. 260–265, 2022. Tersedia: https://scholar.ummetro.ac.id/index.php/IlmuKomputer/article/download/1918/932. [Diakses: 16-Juni-2022]

[10] F. N. Hulu dan M. Putri, "Metode Analisis Enkripsi Dan Dekripsi Dengan Penerapan Algoritma Kriptografi Klasik Ke Dalam Cipher," Jurnal Elektro dan Telkomunikasi, vol. 8, no. 1, pp. 26–34, 2022. Tersedia: https://journal.pancabudi.ac.id/index.php/elektrotelkomunikasi/article/view/4093. [Diakses: 16-Juni-2022]

[11] M. F. Bahari, "Analisa Dan Implemntasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response," Jurnal Sains Dan Teknologi Informasi, vol. 1, no. 2, pp. 49–53, 2022, E-ISSN : 2809-610X. Tersedia: http://ejurnal.seminar-id.com/index.php /jussi/article/view/1442/915. [Diakses: 16-Juni-2022]

[12] P. G. Pamungkas dan A. H. Muhammad, "Modifikasi Algoritma Kriptografi Caesar Chipper Pada Deretan Simbol dan Huruf di Smartphone dan Laptop," Journal Of Information Technologi, vol. 2, no. 1, pp. 16–22, 2022. Tersedia: https://journal.shantibhuana.ac.id/index.php/jifotech/article/view/234/167. [Diakses: 16-Juni-2022]

[13] A. I. Warnilah dan S. N. Nugraha, "Komparasi Algoritma Kriptografi Elgamal dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan," Indonesian Journal On Computer and Information Technologi, vol. 3, no. 2, pp. 243–252, 2018. Tersedia: https://ejournal.bsi.ac.id/ejurnal/index.php/ijcit/article/view/4671. [Diakses: 15-Juni-2022]

[14] R. Latifah, S. N. Ambo dan S. I. Kurnia, "Modifikasi Algoritma Caesar Cipher Dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik Dan Karakter Khusus," Seminar Nasional Sains dan Teknologi, 2017. Tersedia: https://jurnal.umj.ac.id/index.php/semnastek/article/view/2012. [Diakses: 15-Juni-2022]

[15] I. G. B. Jawi dan H. Supriyono, "Pemindaian QR Code Untuk Aplikasi Penampilan Informasi Data Koleksi Di Museum Sangiran Sragen Berbasis Android," Emitor: Jurnal Teknik Elektro, vol. 17, no. 1, pp. 6–8, 2017. Tersedia: https://journals.ums.ac.id/ index.php/emitor/issue/view/712. [Diakses: 17-Juni-2022]

[16] A. Priyambodo, K. Usman dan L. Novamizanti, "Implementasi QR Code Berbasis Android Pada Sistem Presensi," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 7, no. 5, pp. 1011–1020, 2019. Tersedia: https://jtiik.ub.ac.id/index.php/jtiik/article/view/2337/pdf. [Diakses: 17-Juni-2022]

[17] C. Nas, "Data Mining Prediksi Minal Calon Mahasiswa Memilih Perguruan Tinggi Menggunakan Algoritma C4.5," Jurnal Manajemen Informatika, vol. 11, no. 2, pp. 131–145, 2021. Tersedia: https://ojs.unikom.ac.id/index.php/jamika/article/view/5506. [Diakses: 20-Juni-2022]