Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 136-147
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis Modifikasi Algoritma Kriptografi Klasik Menggunakan Algoritma Blum-Micali Generator

Soeb Aripin[1], Muhammad Syahrizal[2]
[1,2]Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Budi Darma, Medan
Jl. Sisingamangaraja No.338,Kota Medan,(061)7875998
e-mail:suefarifin@gmail.com, syahrizal83.budidarma@gmail.com

Abstract

Classical cryptography is the science of securing secret messages (plaintext) into disguised messages (ciphertext) in which each character is changed. The process of converting plaintext into ciphertext is called encryption, while the reverse process is called decryption. However, this classical crypto algorithm can still be solved using the Kasiski method, due to the mathematically regular pattern of repeating keywords. Therefore, in order not to be easily solved, another method is needed, namely by modifying the Caesar Cipher and Vigenere Cipher cryptographic algorithms. Therefore, to strengthen the security of the classical cryptography algorithm, it is necessary to carry out a modification process using an algorithm that is able to change the complexity of the encoding by using a randomization algorithm. By including a randomization algorithm, it is considered that it can eliminate the possibility of attackers guessing the results by knowing the algorithm used. The randomization algorithm used is the Blum-Micali Generator algorithm. The purpose of using the Blum-Micali Generator algorithm is that the encryption process is randomized so that the encryption results obtained are more difficult to guess, making it difficult for cryptanalysts to read the message or information.

Keywords*: Cryptography, Classic, Modification, Blum-Micali Generator*

Abstrak

Kriptografi klasik merupakan ilmu untuk mengamankan pesan rahasia (plainteks) menjadi pesan tersamarkan (cipherteks) yang dalam prosesnya dilakukan pengubahan tiap karakter. Proses mengubah plainteks menjadi cipherteks disebut enkripsi, sementara proses sebaliknya disebut dekripsi. Namun pada algoritma kripto klasik ini masih dapat dipecahkan dengan metode Kasiski, dikarenakan pola perulangan kata kunci yang teratur secara matematis .Oleh sebab itu masih agar tidak mudah dipecahkan diperlukanya suatu cara lain yaitu dengan melakukan modifikasi algoritma kiriptografi Caesar Cipher dan Vigenere Cipher. Oleh sebab itu untuk meperkuat keamanan dari algoritma riptografi klasik perlu dilakukan peroses modifikas dilakukan dengan menggunkana algoritma yang mampu merubah kerumitan penyandian dengan menggunakan algoritma pengacakan. Dengan memasukkan algoritma pengacakan, dianggap dapat menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritma yang digunakan. Adapun algoritma pengacakan yang di gunakan adalah algoritma Blum-Micali Generator. Tujuan dalam menggunakan algoritma Algoritma Blum-Micali Generator adalah proses enkripsi dilakukan pengacakan yang agar hasil enkripasi yang didapatkan lebih sulit ditebak sehingga mempersulit kriptanalis dalam membaca pesan atau informasi tersebut.

Kata kunci*: Kriptografi, Klasik, Modifikasi, Blum-Micali Generator*

1. PENDAHULUAN

Pada zaman yang lebih modern, ilmu keamanan data saat ini sudah dikenal dengan kriptografi. Pada masa modren data telah diolah dengan komputer (secara komputerisasi), kriptografi juga ikut berkembang.

Kriptografi yang sebelumnya hanya diterapkan secara tradisional, kini sudah berkembang dengan melibatkan perhitungan matematika dan teori bilangan dalam pembangkitan kunci, proses enkripsi dan dekripsinya. Walaupun begitu, kriptografi klasik masih banyak digemari oleh kriptografer karena kesederhanaannya dalam enkripsi dan dekripsi pesan[1]. Kriptografi klasik merupakan ilmu untuk mengamankan pesan rahasia (plainteks) menjadi pesan tersamarkan (cipherteks) yang dalam prosesnya dilakukan pengubahan tiap karakter. Proses mengubah plainteks menjadi cipherteks disebut enkripsi, sementara proses sebaliknya disebut dekripsi. Terdapat algoritma monoalfabetik cipher, yaitu algoritma yang mengubah setiap huruf plainteks dipasangkan secara bijektif dengan satu huruf tertentu di cipherteks. Kelemahan algoritma ini yaitu aturan enkripsi dapat diterka dengan analisis frekuensi kemunculan huruf[2]. Sementara itu pada polialfabetik cipher, algoritma yang memungkinkan huruf yang sama akan dienkripsi menjadi huruf yang berbeda. Salah satunya Vigenere cipher, menggunakan kata kunci yang dapat diulang untuk dijumlahkan dengan plainteks dalam perhitungan modulo bilangan bulat[3]. Namun algoritma ini masih dapat dipecahkan dengan metode Kasiski, dikarenakan pola perulangan kata kunci yang teratur secara matematis[4]. Oleh sebab itu masih agar tidak mudah dipecahkan diperlukanya suatu cara lain yaitu dengan melakukan modifikasi algoritma kiriptografi Caesar Cipher dan Vigenere Cipher.

Oleh sebab itu untuk meperkuat keamanan dari algoritma kriptografi klasik perlu dilakukan peroses modifikas dilakukan dengan menggunkana algoritma yang mampu merubah kerumitan penyandian dengan menggunakan algoritma pengacakan. Dengan memasukkan algoritma pengacakan, dianggap dapat menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritma yang digunakan. Telah banyak algoritma bilangan acak yang diusulkan dan digunakan hingga saat ini. Algoritma-algoritma tersebut menggunakan berbagai pendekatan berbeda untuk menghasilkan bilangan acak seacak mungkin. Adapun salah satu algoritma pengacakan yang di gunakan adalah algoritma Blum-Micali Generator. Algoritma Blum-Micali Generator adalah algoritma yang menghasilkan urutan angka yang secara statistik independen dan tidak dapat ditebak berdasarkan tingkat kesulitan untuk menghitung logaritma diskrit, yang berdasarkan kepercayaan bahwa modular eksponensiasi modulo adalah prima dan fungsi satu arah[5]. Tujuan dalam menggunakan algoritma Blum-Micali Generator adalah proses enkripsi dilakukan pengacakan yang agar hasil enkripasi yang didapatkan lebih sulit ditebak sehingga mempersulit kriptanalis dalam membaca pesan atau informasi tersebut. Dengan demikian ukuran tingkat keamanan menjadi lebih tinggi dari monoalfabetik cipher karena tidak dapat dideteksi dengan analisis frekuensi kemunculan huruf, dan juga lebih aman dari Vigenere Cipher karena ukuran kata kunci lebih sulit.

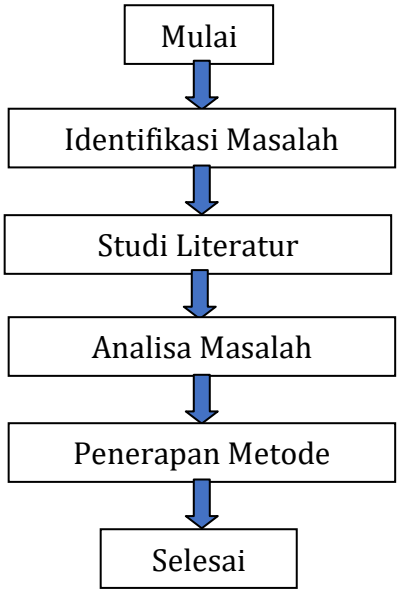
2. METODOLOGI PENELITIAN

2.1. Tahapan Penelitian

Di bagian tahapan penelitian dalam analisis modifikasi algoritma kriptografi klasik menggunakan algoritma Blum-Micali Generator yaitu:

a) Identifikasi masalah, pada tahapan ini dilakukan untuk mengetahui permasalahan dan metode yang digunakan pada penelitian ini.
b) Studi literatur, ditahap ini penulis mempelajari beberapa kajian literatur terkait dengan penelitian yang telah dibuat oleh beberapa orang sebelumnya termasuk juga mempelajari jurnal-jurnal atau buku-buku yang berkaitan dengan kriftografi klasik dan pengacakan.
c) Analisa masalah, pada tahap analisa ini penulis melakukan pengumpulan data, mempelajari dan melakukan perumusan demi mendukung penelitian ini dalam melakukan proses pengolahan data.
d) Penerapan metode, tahap ini merupakan tahap modifikasi algoritma kriptografi klasik menggunakan algoritma Blum-Micali Generator.

Dari beberapa tahapan diatas dapat digambarkan seperti bagan dibawah ini :



Gambar 1. Tahapan Penelitian

2.2. Kriptografi Klasik

Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini sudah digunakan beberapa abad yang lalu[6]. Kriptografi ini melakukan pengacakan huruf pada kata terang / plaintext. Kriptografi ini hanya melakukan pengacakan pada huruf A – Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern[7].

2.3. Algoritma Caesar Cipher

Caesar cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada cipherteks[8]. Teknik seperti ini disebut juga sebagai cipher abjad tunggal. Adapun langkah-langkah yang dilakukan untuk membentuk cipherteks dengan Caesar cipher adalah[9]:

a) Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
b) Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya[2].

2.4. Algoritma Vigenere Cipher

Vigenere cipher adalah metode mengenkripsi teksalfabet dengan menggunakan serangkaian caesar cipheryang berbeda berdasarkan huruf dari kata kunci danmerupakan bentuk substitusi polyalphabetic yang sederhana. Karakter yang digunakan dalam VigenereCipher yaitu A, B, C, ..., Z dan dikonversi kedalam angka0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menuliskunci berulang kali sesuai dengan panjang karakter pada pesan . [10]. Model matematika dari enkripsi dan dekripsi pada algoritma vigenere cipher adalah seperti berikut:

$Ci = (Pi + Ki) \bmod 26$ (1)

Sedangkan untuk proses dekripsi adalah:

$Pi = (Ci - Ki) \bmod 26$ jika $Ci-Ki > 0$ (2)

$Pi = ((Ci - Ki) + 26) \bmod 26$ jika $Ci-Ki < 0$ (3)

Keterangan:
C = Ciphertext (Pesan Acak)
P = Plaintext (Pesan Asli)
K = Kunci

2.5. Algoritma Vigenere Cipher

Algoritma Blum-Micali Generator adalah algoritma yang menghasilkan urutan angka yang secara statistik independen dan tidak dapat ditebak berdasarkan tingkat kesulitan untuk menghitung logaritma diskrit, yang berdasarkan kepercayaan bahwa modular eksponensiasi modulo adalah prima dan fungsi satu arah[5]. Algoritma Blum-Micali adalah pembangkit bilangan acak semu cryptographically aman. Algoritma mendapatkan keamanannya dari kesulitan menghitung logaritma diskrit. Berdasarkan tingkat kesulitan untuk menghitung logaritma diskrit, yang berdasarkan kepercayaan bahwa modular eksponensiasi modulo adalah prima dan fungsi satu arah. Bentuk umum BM:

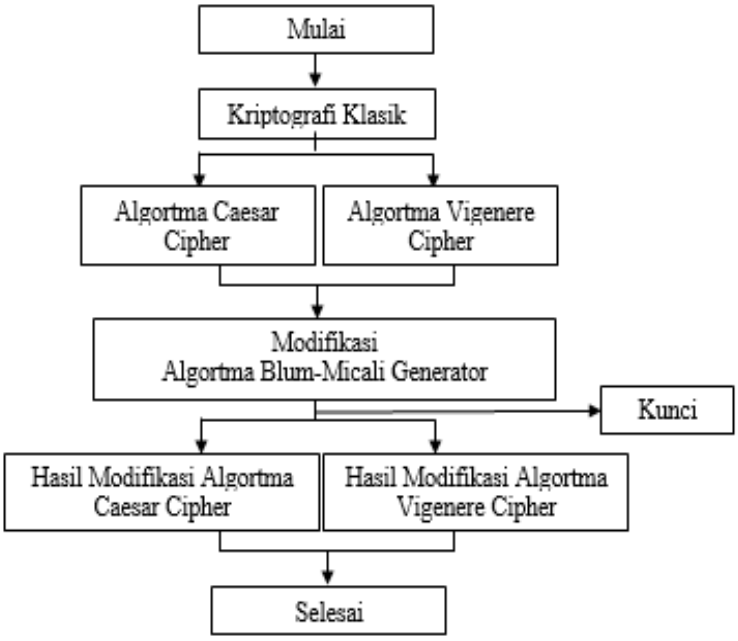
$X_{i+1} = aX_i \bmod m, i \geq 0$ (4)

Output dari generator adalah 1 jika Xi < m/2, selain itu menghasilkan 0

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Sebagai langkah awal yang dilakukan agar dapat mengetahui gambaran permasalahan adalah dengan melakukan analisis permasalahan. Untuk mengananalisis memodifikasi algoritma kriptografi klasik menggunakan algoritma blum-micali generator. Dimana proses modifikasi dengan algoritma Blum-Micali Generator dengan cara proses enkripsi dilakukan pengacakan yang agar hasil enkripasi yang didapatkan lebih sulit ditebak sehingga mempersulit kriptanalis dalam membaca pesan atau informasi tersebut. Dengan demikian ukuran tingkat keamanan menjadi lebih tinggi dari monoalfabetik cipher karena tidak dapat dideteksi dengan analisis frekuensi kemunculan huruf, dan juga lebih aman dari Vigenere Cipher karena ukuran kata kunci lebih sulit. Secara garis besar, proses yang dilakukan pada penelitian ini digambarkan dengan block diagram berikut:



Gambar 2. Proses Modifikasi Kriptografi Klasik

3.2. Modifikasi Algoritma Caesar Cipher

Modifikasi algoritma Caesar Cipher dilakukan dengan menggunakan algoritma bilangan random dengan cara melakuakn pengacakan kunci, dianggap dapat menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritmanya. Telah banyak algoritma generator bilangan acak yang diusulkan dan digunakan hingga saat ini. Algoritma-algoritma tersebut menggunakan berbagai pendekatan berbeda untuk menghasilkan bilangan random seacak. Salah satu algoritma tersebut adalah

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 136-147
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

algoritma Blum-Micali Generator. Proses yang dilakuakan untuk memodifikasi algorima algoritma Caesar Cipher adalah sebagai berikut:

Adapun sampel penerapan untuk modifikasi algorima caesar cipher dengan algoritma Blum-Micali Generator, dimisalkan plainteks "**UNIVERSITAS BUDI DARMA"** dan Kunci "**BEOS NIFIRA"** Proses yang dilakuakan untuk memodifikasi algorima algoritma Caesar Cipher adalah sebagai berikut:

1) Proses Pembentukan Kunci Dengan menggunkan Blum-Micali Generator
   Pada Algoritma Caesar Cipher kunci atau key yang digunakan adalah hasil nilai pengacakan yang nilai asci dari karakter kunci yang diberikan, adapun penyelesaiyanya sebagai berikut:
   Kunci : **BEOS NIFIRA**
   a) Rubah karakter kunci kenilai desimal

Teks	B	E	O	S	Spasi	N	I	F	I	R	A
DEC	66	69	79	83	32	78	73	70	73	82	65

   b) Ambil nilai kunci berdasarkan hasil pengacakan dengan menerapkan algoritma Blum-Micali Generator dengan nilai denga nilai Xi= 11 m=255 berdasarkan rumus 7 sebagai berikut:
   X_1 = 66*11 mod 255
   X_1 =216
   Sehingga didaptkan hasil dari pengacangan dengan algoritma Blum-Micali Generator sebagai berikut

Teks	B	E	O	S	Spasi	N	I	F	I	R	A
DEC	66	69	79	83	32	78	73	70	73	82	65
BCG	216	114	81	93	171	78	84	15	75	30	165

   Sehingga didapatkan hasil kunci nya yaitu:
   Kunci BCG 216 114 81 93 171 78 84 15 75 30 165
2) Proses Enkripsi dengan menggunakan Algoritma Caesar Cipher
   Plaintext: **UNIVERSITAS BUDI DARMA**
   Kunci hasil Blum-Micali Generator : (216), (114), (81), (93), (171), (78), (84), (15), (75), (30), (165)
   Adapun peroses enkripsi dengan menggunakan Algoritma Caesar Cipher berdasarkan rumus 4 yaitu:
   a) Rubah karakter Plaintekt kenilai desimal

Plainteks	**U**	**N**	**I**	**V**	**S**	**I**	**T**	**A**	**S**	**B**	**U**	**D**	**I**	**D**	**A**	**R**	**M**	**A**
DEC	**85**	**78**	**73**	**86**	**83**	**73**	**84**	**65**	**83**	**66**	**85**	**68**	**73**	**68**	**65**	**82**	**77**	**65**
Kunci	**216**	**114**	**81**	**93**	**171**	**78**	**84**	**15**	**75**	**30**	**165**							

   b) Poses Enkripsi dengan nilai plainteks maka kunci diulang sesuai jumlah plainteks dan nilai modulus 255 sesui jumlah karakter ASC:

Plainteks	**U**	**N**	**I**	**V**	**S**	**I**	**T**	**A**	**S**	**B**	**U**	**D**	**I**	**D**	**A**	**R**	**M**	**A**
DEC	**85**	**78**	**73**	**86**	**83**	**73**	**84**	**65**	**83**	**66**	**85**	**68**	**73**	**68**	**65**	**82**	**77**	**65**
Kunci	**216**	**114**	**81**	**93**	**171**	**78**	**84**	**15**	**75**	**30**	**165**	**216**	**114**	**81**	**93**	**171**	**78**	**84**

   Ci = (Pi + Ki) mod M
   C_1 = (U + 216) mod 256
   C_1 = (85 + 216) mod 256

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 136-147
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

$C_1 = 46 \rightarrow$ **.**
……
$C_{18} = (A + 15) \bmod 256$
$C_{18} = (65 + 15) \bmod 256$
$C_{18} = 80 \rightarrow$ **P**

Adapun hasil dari enkripsi sebagai berikut:

Plainteks	**U**	**N**	**I**	**V**	**S**	**I**	**T**	**A**	**S**	**B**	**U**	**D**	**I**	**D**	**A**	**R**	**M**	**A**
DEC	**85**	**78**	**73**	**86**	**83**	**73**	**84**	**65**	**83**	**66**	**85**	**68**	**73**	**68**	**65**	**82**	**77**	**65**
Kunci	**216**	**114**	**81**	**93**	**171**	**78**	**84**	**15**	**75**	**30**	**165**	**216**	**114**	**81**	**93**	**171**	**78**	**84**
Enkripsi	**.**	**└**	**Ü**	**▒**	**▪**	**Ú**	**¿**	**P**	**ˣ**	**`**	**·**	**¸**	**┤**	**Ó**	**ˣ**	**²**	**Ø**	**Ó**
DEC	46	192	154	179	254	151	168	80	158	96	250	29	187	149	158	253	155	149

Hasil Enkripsi : **. └Ü▒▪Ú¿Pˣ`·¸┤Óˣ²ØÓ**

3) Proses Dekripsi dengan menggunakan Algoritma Caesar Cipher

Enkripsi : . └Ü▒▪Ú¿Pˣ`·¸┤Óˣ²ØÓ

Kunci : (216), (114), (81), (93), (171), (78), (84), (15), (75), (30), (165)

Adapun peroses Deskripsi dengan menggunakan Algoritma Caesar Cipher berdasarkan rumus 4 dan 5 yaitu:

a) Rubah karakter enkripsi kenilai desimal

Enkripsi	.	└	Ü	▒	▪	Ú	¿	P	ˣ	`	·	¸	┤	Ó	ˣ	²	Ø	Ó
DEC	46	192	154	179	254	151	168	80	158	96	250	29	187	149	158	253	155	149
Kunci	216	114	81	93	171	78	84	15	75	30	165	216	114	81	93	171	78	84

b) Proses deskripsi sebagai berikut:

Pi = (Ci – Ki) mod m jika Ci-Ki > 0
Pi = ((Ci - Ki) + m) mod m jika Ci-Ki < 0

1. Ci-Ki < 0
   $P_1 = ((46-216) + 255) \bmod 255$
   $P_1 = 85 \bmod 255$
   $P_1 = 85 \rightarrow$ **U**
   ……..
18. Ci-Ki > 0
   $P_{18} = ((149-84) \bmod 255$
   $P_{18} = 78 \bmod 255$
   $P_{18} = 65 \rightarrow$ **A**

Adapun hasil dari Deskripsi sebagai berikut:

Enkripsi	.	└	Ü	▒	▪	Ú	¿	P	ˣ	`	·	¸	┤	Ó	ˣ	²	Ø	Ó
DEC	46	192	154	179	254	151	168	80	158	96	250	29	187	149	158	253	155	149
Kunci	216	114	81	93	171	78	84	15	75	30	165	216	114	81	93	171	78	84
Deskripsi	U	N	I	V	S	I	T	A	S	B	U	D	I	D	A	R	M	A
DEC	85	78	73	86	83	73	84	65	83	66	85	68	73	68	65	82	77	65

Berdasarkan hasil kesimpulan dari proses enkripsi dan deskripsi dapat disimpulakan bahwasannya modifikasi algoritma Caesar Cipher dengan

algoritma Blum-Micali Generator dapat dilakukann karena plainteks yang di enkripsi dapat di deskripsikan kembali

3.3. Modifikasi Algoritma Vigenere Cipher

Modifikasi algoritma Vigenere Cipher dilakukan dengan cara yang sama seperti modifikasi caesat ciper dengan menggunakan algoritma bilangan random dengan cara melakuakn pengacakan kunci, dianggap dapat menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritmanya. Adapun sampel penerapan untuk modifikasi algorima vigenere cipher dengan algoritma Blum-Micali Generator, dimisalkan plainteks "**UNIVERSITAS BUDI DARMA"** dan Kunci "**BEOS NIFIRA"** adapun prosesnya sebagai berikut:

1) Proses Pembentukan Kunci Dengan menggunkan Blum-Micali Generator
   Pada algoritma vigenere cipher kunci atau key yang digunakan adalah hasil nilai pengacakan yang nilai asci yang paling banyanya muncul dari karakter kunci yang diberikan, adapun penyelesaiyanya sebagai berikut:
   Kunci : **BEOS NIFIRA**
   a) Rubah karakter kunci kenilai desimal berdasarkan tabel 2.1 substitusi algoritma vigenere cipher kunci

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

   Sehinnga diubah kenilai indek subtitusi substitusi algoritma vigenere cipher kunci

Teks	B	E	O	S	N	I	F	I	R	A
DEC	1	4	14	18	13	8	5	8	17	0

   b) Ambil nilai kunci berdasarkan hasil pengacakan dengan menerapkan algoritma Blum-Micali Generator dengan nilai denga nilai Xi= 10 m=26 berdasarkan rumus 7 sebagai berikut:
   X_1 = 1*10 mod 26
   X_1 =10

   X_{10}= 0*10 mod 26
   X_{10} =0
   Sehingga didaptkan hasil dari pengacangan dengan algoritma Blum-Micali Generator sebagai berikut

Teks	B	E	O	S	N	I	F	I	R	A
DEC	1	4	14	18	13	8	5	8	17	0
BCG	10	14	24	2	23	18	15	18	1	0

   Sehingga didapatkan hasil kunci nya yaitu:
   Kunci BCG 10 14 24 2 23 18 15 18 1 0
2) Proses Enkripsi dengan menggunakan Algoritma Vigenere Ciphe
   Plaintext: **UNIVERSITAS BUDI DARMA**

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 136-147
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Kunci hasil Blum-Micali Generator : (10), (14), (24), (2), (23), (18), (15), (18), (1), (0)

Adapun peroses enkripsi dengan menggunakan Algoritma Vigeneri Cipher berdasarkan rumus 1 yaitu:

a) Rubah karakter Plaintekt kenilai tabel 2.1 substitusi algoritma vigenere cipher kunci

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

Hasilnya sebagai berikut:

Plainteks	U	N	I	V	S	I	T	A	S	B	U	D	I	D	A	R	M	A
Indeks	20	13	8	21	18	8	19	0	18	1	20	3	8	3	0	17	12	0
Kunci	10	14	24	2	23	18	15	18	1	0								

b) Poses Enkripsi dengan nilai plainteks maka kunci diulang sesuai jumlah plainteks:

Plainteks	U	N	I	V	S	I	T	A	S	B	U	D	I	D	A	R	M	A
Indeks	20	13	8	21	18	8	19	0	18	1	20	3	8	3	0	17	12	0
Kunci	10	14	24	2	23	18	15	18	1	0	10	14	24	2	23	18	15	18

$C_i = (P_i + K_i) \bmod 26$
$C_1 = (P_1 + K_1) \bmod 26$
$C_1 = (20 + 10) \bmod 26$
$C_1 = 30 \bmod 26$
$C_1 = 4 \rightarrow$ **E**

$C_{18} = (P_{18} + K_{18}) \bmod 26$
$C_{18} = (0+18) \bmod 26$
$C_{18} = 18 \bmod 26$
$C_{18} = 18 \rightarrow$ **S**

Sehingga didapaktkan hasil dari enkripsi algoritma Vigeneri Cipher sebegai berikut:

Plainteks	U	N	I	V	S	I	T	A	S	B	U	D	I	D	A	R	M	A
Indeks	20	13	8	21	18	8	19	0	18	1	20	3	8	3	0	17	12	0
Kunci	10	14	24	2	23	18	15	18	1	0	10	14	24	2	23	18	15	18
Enkripsi	E	B	G	X	P	A	I	S	T	B	E	R	G	F	X	J	B	S
Indeks	4	1	6	23	15	0	8	18	19	1	4	17	6	5	23	9	1	18

Hasil Enkripsi = **E B G X P A I S T B E R G F X J B S**

3) Proses Dekripsi dengan menggunakan Algoritma Vigenere Ciphe

Enkripsi : E B G X P A I S T B E R G F X J B S
Kunci : (10), (14), (24), (2), (23), (18), (15), (18), (1), (0)

Adapun peroses enkripsi dengan menggunakan Algoritma Vigeneri Cipher berdasarkan rumus 2 yaitu:

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 136-147
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

a) Rubah karakter Enkripsi kenilai tabel 2.1 substitusi algoritma vigenere cipher kunci

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

Hasilnya sebagai berikut:

Enkripsi	E	B	G	X	P	A	I	S	T	B	E	R	G	F	X	J	B	S
Indeks	4	1	6	23	15	0	8	18	19	1	4	17	6	5	23	9	1	18
Kunci	10	14	24	2	23	18	15	18	1	0								

b) Poses deskripsi dengan nilai hasil enkripsi maka kunci diulang sesuai jumlah plainteks:

Enkripsi	E	B	G	X	P	A	I	S	T	B	E	R	G	F	X	J	B	S
Indeks	4	1	6	23	15	0	8	18	19	1	4	17	6	5	23	9	1	18
Kunci	10	14	24	2	23	18	15	18	1	0	10	14	24	2	23	18	15	18

$P_i = (C_i - K_i) \bmod 26$
$P_1 = (C_1 - 10) \bmod 26$
$P_1 = (4 - 10) \bmod 26$
Karena hasil P_1 tidak dapat di cari maka lakukan berdasarkan rumus 3 sebagai berikut:
$P_1 = ((C_1 + K_1) + M) \bmod 26$
$P_1 = (4 -10) +26) \bmod 26$
$P_1 = 20 \bmod 26$
$P_1 = 20 \rightarrow$ **U**

$P_{18} = (P_{18} - K_{18}) \bmod 26$
$P_{18} = (18-18) \bmod 26$
$P_{18} = 0 \bmod 26$
$P_{18} = 0 \rightarrow$ **A**

Sehingga didapaktkan hasil dari Deskripsi algoritma Vigeneri Cipher sebegai berikut:

Enkripsi	E	B	G	X	P	A	I	S	T	B	E	R	G	F	X	J	B	S
Indeks	4	1	6	23	15	0	8	18	19	1	4	17	6	5	23	9	1	18
Kunci	10	14	24	2	23	18	15	18	1	0	10	14	24	2	23	18	15	18
Deskripsi	U	N	I	V	S	I	T	A	S	B	U	D	I	D	A	R	M	A
Indeks	20	13	8	21	18	8	19	0	18	1	20	3	8	3	0	17	12	0

Berdasarkan hasil kesimpulan dari proses enkripsi dan deskripsi dapat disimpulakan bahwasannya modifikasi algoritma Vigeneri Cipher dengan algoritma Blum-Micali Generator dapat dilakukann karena plainteks yang di enkripsi dapat di deskripsikan kembali.

3.4. Hasil Perbandingan Modifikasi Kriptografi Klasik

Berdasarkan pengujian modifikasi kiriftografi klasik dengan algoritma algoritma Blum-Micali Generator dengan 2 sampel algoritma kiriftografi klasik yaitu Algoritma Vigeneri Cipher dan Caesar Cipher. Hasil analisa kedua metode tersebut bahwa proses enkripsi dan deskripsi dengan memodifikasi menggunakan algoritma Blum-Micali Generator dapat dilakukann karena plainteks yang di enkripsi dapat di deskripsikan kembali. Hasil dari pengujian nampat terlihat jelas dimana dari hasil memiliki tingkat perbedaan yang sangat jelas dari hasil enkripsi dan dapat dilihat di tabel dibawah ini:

Tabel 1. Hasil Perbandingan

Plainteks	Algoritma	Hasil Enkripsi	Hasil Enkripsi Modifikasi BMG
UNIVERSITAS BUDI DARMA	Caesar Cipher	**T M H U D Q R H S @ R A T C H C @ Q L @**	**. └ Ü ▒ ▪ Ú ¿ P ˣ ` · ¸ | Ó ˣ ² Ø Ó**
	Vigeneri Cipher	**V O J W F S T J U B T C V E J E B S N B**	**E B G X P A I S T B E R G F X J B S**

4. SIMPULAN

Setelah dilakukan pengimplementasian mengananalisis memodifikasi algoritma kriptografi klasik menggunakan algoritma blum-micali generator, maka dapat diambil kesimpulan dimana, pengujian modifikasi kiriftografi klasik dengan algoritma Blum-Micali Generator dengan 2 sampel algoritma kiriftografi klasik yaitu Algoritma Vigeneri Cipher dan Caesar Cipher. Hasil analisa kedua metode tersebut bahwa proses enkripsi dan deskripsi dengan memodifikasi menggunakan algoritma Blum-Micali Generator dapat dilakukann karena plainteks yang di enkripsi dapat di deskripsikan kembali. Hasil dari pengujian nampat terlihat jelas memiliki tingkat perbedaan dari hasil enkripsi.

DAFTAR PUSTAKA

[1] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 61–64, 2016.

[2] E. Endaryono, "Perancangan Simulasi Metode Caesar Cipher Menggunakan Microsoft Excel – Alternatif Media Pembelajaran Kriptografi," *SAP (Susunan Artik. Pendidikan)*, vol. 4, no. 3, 2020.

[3] M. Ramli, R. Asri, and M. Zarlis, "Implementasi Algoritma Vigenere Subtitusi dengan Shift Indeks Prima," *Semin. Nas. Teknol. Inform.*, pp. 149–154, 2017.

[4] A. Wijaya, "Modifikasi Algoritma Kriptografi Klasik dengan Implementasi Deterministic Finite Automata melalui Partisi Pesan Asli berdasarkan Kriteria Pesan Bagian," *J. Sci. Appl. Technol.*, vol. 4, no. 2, p. 133, 2020.

[5] A. Josefin and M. Andersen, "Provably Secure Pseudo-Random

Generators," in *A Literary Study*, 2013, pp. 1–24.
[6] D. Ariyus, "Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi.," in *Journal of Chemical Information and Modeling*, 2008.
[7] R. Sadikin, *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: C.V Andi Offset, 2012.
[8] Jamaludin and Romindo, *Kriptografi: Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA*. 2020.
[9] D. Rachmawati and A. Candra, "Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks," *J. Edukasi dan Penelit. Inform.*, 2015.
[10] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.