

Peningkatan Ketahanan Algoritma Vigenere menggunakan Generator kunci Tiga Lapis

Edy Supriyanto¹, Widiyanto Tri Handoko², Sutrasno Andre Wibowo^{3*}, Eka Ardhianto⁴

^{1,2,3,4}Fakultas Teknologi Informasi dan Industri, Universitas Stikubank

¹edy_supriyanto@edu.unisbank.ac.id, ²wthandoko@edu.unisbank.ac.id,
³andresutrasno381@gmail.com, ⁴ekaardhianto@edu.unisbank.ac.id

Abstract

Vigenere is a simple text-based encryption algorithm. In cryptography, vigenere has been modified to strengthen the confidentiality of information from unauthorized parties. Important factors that affect the use of keys. This study aims to strengthen the resilience of available information through the key generating process. This experiment proposes the use of a multi-layer key generating technique. The random function, the use of Euler numbers and the method of issuing the Blum Blum Shub key were experimented with the "extended Vigenere" encryption model. As a metric used to calculate the entropy value. This experiment resulted in the use of multi-layered key generation in the "extended Vigenere" encryption model, increasing the entropy value of confidential information which resulted in increased resilience from cryptanalytic attacks.

Keywords : Entropy, Information, Key, Vigenere

Abstrak

Vigenere merupakan algoritma enkripsi berbasis teks yang sederhana. Dalam kriptografi, vigenere telah mengalami banyak modifikasi untuk memperkuat kerahasiaan informasi dari pihak yang tidak berhak. Faktor penting yang mempengaruhi ialah penggunaan kunci. Penelitian ini bertujuan untuk memperkuat ketahanan informasi yang diamankan vigenere melalui proses penerbitan kunci. Eksperimen ini mengusulkan penggunaan Teknik penerbitan kunci secara berlapis. Fungsi random, penggunaan bilangan euler dan metode penerbitan kunci Blum Blum Shub dieksperimenkan pada model enkripsi "extended Vigenere". Sebagai metrik performasi digunakan perhitungan nilai entropi. Eksperimen ini mendapatkan hasil berupa penggunaan penerbitan kunci secara berlapis pada model enkripsi "extended Vigenere" meningkatkan nilai entropi informasi rahasia yang berimbas pada peningkatan ketahanan informasi dari serangan kriptanalis.

Kata Kunci : Entropi, Informasi, Kunci, Vigenere.

Pendahuluan

Pertukaran informasi merupakan pokok kegiatan dalam komunikasi dunia digital. Teks, suara dan gambar adalah format digital dalam percakapan publik, pribadi atau komunikasi dalam bentuk lain (Ahamed & Krishnamoorthy, 2020). Informasi dapat bersifat umum dan khusus. Informasi yang disampaikan secara umum tentunya akan diakses banyak entitas secara bebas, berbeda dengan informasi khusus yang hanya dapat diakses oleh pihak pihak tertentu saja sehingga perlu benar benar dijaga kerahasiannya. Aspek penting dalam menjaga keamanan informasi dikenal sebagai *confidentiality*. *Confidentiality* informasi dapat diselesaikan dengan menerapkan proses kriptografi (Rahmah Zagi Asst Abeer Tariq Maolood, 2021). Kriptografi bertujuan untuk menjaga kerahasiaan informasi (Politeknik Ganesha Medan, 2020). Proses kriptografi ialah menghasilkan teks sandi (cipherteks) dari informasi berupa teks biasa (plainteks) menggunakan kunci (*password*), sehingga informasi dari keadaan yang dapat dibaca menjadi yang tidak dapat dipahami melalui proses enkripsi (Ahamed & Krishnamoorthy, 2020). Plainteks ialah informasi yang menggunakan bahasa normal untuk komunikasi, sedangkan cipherteks ialah pesan yang sudah menjadi teks sandi (Nahar & Chakraborty, 2020). Enkripsi ialah proses mengatur ulang pesan asli ke dalam format yang tidak dapat dikenali (Fauzi & Theophilus, 2021) dengan pengertian lain mengubah data asli (plaintext) menjadi data samar (ciphertext) yang telah teracak sedemikian rupa hingga sulit dimengerti oleh pihak lain (Fauzi & Theophilus, 2021), sedangkan cara untuk mendapatkan kembali pesan sebelumnya

disebut sebagai dekripsi (Nahar & Chakraborty, 2020) dengan pengetahuan lain proses yang mengubah kembali data samar (ciphertext) menjadi data asli (plaintext) (Fauzi & Theophilus, 2021).

Vigenere cipher atau dikenal sebagai algoritma vigenere merupakan salah satu model Teknik kriptografi yang dikenalkan pada tahun 1500-an. Pada masa itu vigenere digunakan untuk memproses pesan berupa teks (Ardhianto et al., 2021). Vigenere merupakan cipher substitusi polialfabet yang menggunakan pemetaan posisi symbol karakter, dimana setiap simbol ditransformasikan oleh salah satu dari beberapa *cipher-shift* yang ditentukan dengan kunci (*key*) (Park et al., 2020). Vigenere memiliki sifat kriptografi simetris, yaitu menggunakan kunci yang sama pada proses enkripsi dan dekripsinya (Ardhianto et al., 2021) , (Purnomo Sidik, 2021). Secara normal, kunci dalam vigenere digunakan secara berulang sepanjang plainteks yang diproses. Proses enkripsi vigenere standar digambarkan serupa dengan Caesar cipher dengan nilai pergeseran simbol yang berbeda, seperti diilustrasikan pada gambar 1. Sebagai contoh, plainteks: ATTACKDOWN dan kunci: LEMON maka akan menghasilkan cipherteks: LXFOPVEFRNHR.

		Plaintext																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

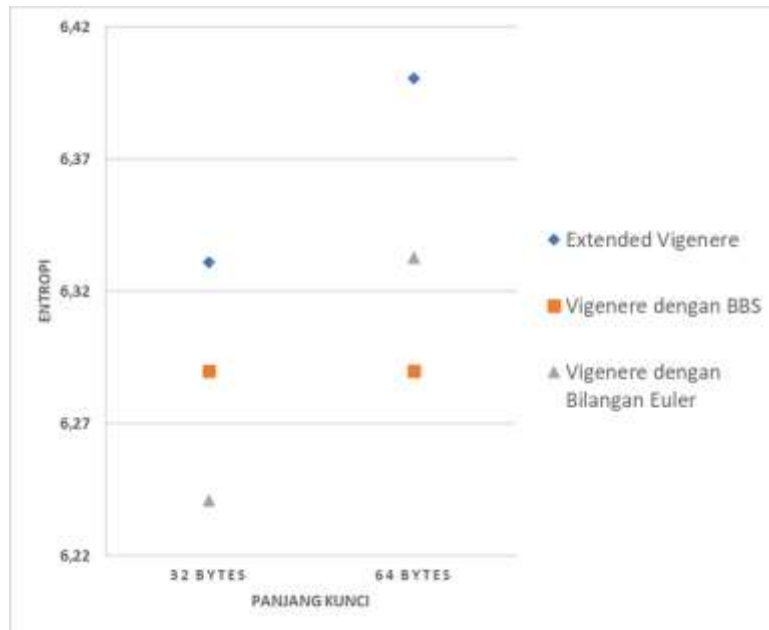
Gambar 1. Table Vigenere Standar

Vigenere mengalami evolusi untuk menutupi kekurangan serta penyesuaian dengan model informasi yang saat ini digunakan. Salah satu evolusi vigenere ialah dengan memodifikasi kunci dan penggunaan karakter set yang diperluas. Kekuatan algoritma kriptografi tergantung pada pengambilan nilai kunci dari ruang domain. Jadi kekuatan algoritma tergantung pada waktu pengambilan kunci (Uniyal et al., 2021). Penggunaan kunci vigenere yang pendek dan berulang akan menyebabkan kerentanan dalam pengamanan informasi (Ardhianto et al., 2021). Modifikasi kunci pada vigenere salah satunya ialah penggunaan *Euler Number* (Ahamed & Krishnamoorthy, 2020). Bilangan Euler diadopsi dalam vigenere cipher memberikan keacakan dalam merahasiakan informasi, sehingga menyulitkan kriptanalisis. Modifikasi kunci lainnya ialah penggunaan pembangkit kunci Blum Blum Shub (Telaumbanua & Zebua, 2020). Modifikasi ini melakukan penerbitan kunci berdasarkan pembangkit kunci Blum Blum Shub (BBS), artinya kunci yang digunakan pada vigenere berdasar dari luaran pembangkit kunci tersebut. Penggunaan Blum Blum Shub ini ditujukan untuk meminimalisir keterkaitan kunci dengan pengirim dan penerima, sehingga akan meminimalkan Tindakan pemecahan kunci (Telaumbanua & Zebua, 2020). Modifikasi vigenere juga dilakukan dengan memperbanyak karakter set menjadi 96 simbol. Modifikasi ini dikenal sebagai *Extended Vigenere*. Modifikasi ini menghasilkan bentuk tabel vigenere dengan ukuran 95x95, lebih besar dibanding vigenere yang asli menggunakan jumlah alfabet 26x26. Modifikasi ini dilakukan dengan tujuan

untuk meningkatkan keamanan informasi dan mempersulit kriptanalisis (Nahar & Chakraborty, 2020). Perluasan karakter set ini juga ditujukan untuk mengadopsi penggunaan simbol-simbol karakter yang saat ini sudah menjadi lebih kompleks seperti huruf kapital, angka, tanda baca dan simbol matematika.

Eksperimen awal dilakukan untuk melihat performa vigenere cipher pada penelitian sebelumnya. Hasil eksperimen awal digunakan sebagai state-of-the-art eksperimen pengembangan. Sampel plainteks diambil dari Astronomer Telegram Dataset. Dataset ini berisi kumpulan informasi singkat tentang pengamatan astronomi. Sample yang digunakan diambil dengan ukuran 1 KB. Panjang kunci yang digunakan pada eksperimen awal ialah 32 Byte dan 64 Byte. Jumlah percobaan pada eksperimen awal ialah sebanyak 25 kali untuk setiap ukuran kunci yang berbeda, sehingga terdapat 100 percobaan. Nilai entropi dihitung sebagai metrik pengukuran. Entropi dihitung dari cipherteks yang dihasilkan. Analisis entropi berguna untuk mengukur tingkat keacakan cipherteks (Susanto et al., 2020). Nilai ideal entropi ialah 8, semakin tinggi nilai entropi pada cipherteks maka akan semakin sulit dipecahkan. Perhitungan entropi dilakukan dengan menggunakan persamaan 1, dengan E ialah nilai entropi, R ialah rentang kode ASCII, $c_{(r)}$ ialah probabilitas symbol pada cipherteks. Visualisasi rata-rata entropi cipherteks yang diperoleh dari setiap percobaan awal diperlihatkan pada gambar 2.

$$E = - \sum_{r=0}^{R=255} c_{(r)} \log_2(c_{(r)})$$



Gambar 2. Nilai Entropi Cipherteks Vigenere Cipher pada eksperimen awal

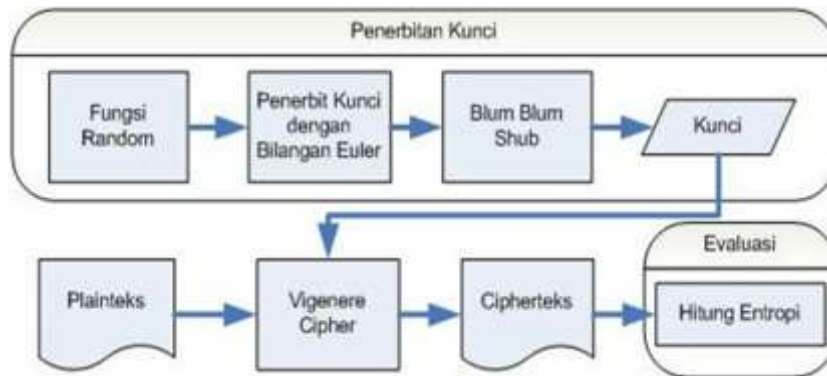
Hasil eksperimen awal yang terlihat pada gambar 2 menunjukkan perbedaan tingkat keamanan informasi yang diukur dengan nilai entropi. Hal ini disebabkan penggunaan penerbitan kunci yang berbeda pada vigenere. Pengembangan vigenere dimotivasi untuk meningkatkan keamanan informasi. Berdasarkan eksperimen awal, salah satu faktor yang penting dalam vigenere untuk meningkatkan tingkat keamanan informasi ialah kunci yang digunakan, oleh karena itu pemilihan kunci yang tepat akan mampu meningkatkan keamanan informasi. Penggunaan kunci pada vigenere merupakan hal yang paling krusial. Kunci vigenere secara umum adalah pendek dan digunakan secara berulang (Qowi & Hudallah, 2021). Penggunaan kunci yang dipilih secara manual juga akan menjadikan kerapuhan dalam vigenere. Selain itu permasalahan distribusi kunci simetris ini akan menimbulkan kecurigaan (Purnomo Sidik, 2021). Terlihat pada gambar 2, modifikasi pada vigenere menghasilkan nilai entropi yang berbeda. Penelitian sebelumnya

menggunakan pembangkit kunci yang berbeda untuk diadopsi pada vigenere. Pertanyaan riset yang muncul dari eksperimen awal ialah bagaimana pengaruh penerbitan kunci pada vigenere yang dilakukan secara berlapis terhadap peningkatan keamanan informasi.

Penelitian ini bertujuan untuk memperkuat ketahanan informasi yang diamankan vigenere melalui proses penerbitan kunci secara berlapis. Penelitian ini dilakukan dengan eksperimen penerbitan kunci vigenere menggunakan fungsi random, bilangan euler dan pembangkit kunci Blum Blum Shub. Hasil penerbitan kunci ini diadopsikan pada model enkripsi extended vigenere dan diukur nilai entropi cipherteksnya..

Metode

Eksperimen mengusulkan penggunaan penerbitan kunci secara berlapis dengan menggunakan fungsi random, bilangan Euler dan Blum Blum Shub sebagai penerbit kunci pada vigenere. Gambar 3 memvisualisasikan usulan desain



Gambar 3 Desain Modifikasi Penerbitan Kunci pada Extended Vigenere

modifikasi penerbitan kunci pada extended vigenere.

Penelitian ini melakukan eksperimen awal dan eksperimen pengembangan. kspirimen awal dilakukan untuk melihat performa algoritma vigenere yang telah dikembangkan (Telaumbanua & Zebua, 2020) , (Nofiyanto et al., 2017) sebagai state-of the art. Nilai yang diperoleh

seperti pada gambar 2 digunakan sebagai pembanding pada nilai eksperimen pengembangan. Eksperimen dilakukan dengan memodifikasi penerbitan kunci pada vigenere secara berlapis.

Eksperimen menggunakan sampel plainteks dari Astronomer Telegram Dataset dengan ukuran 1 KB. Sampel ini

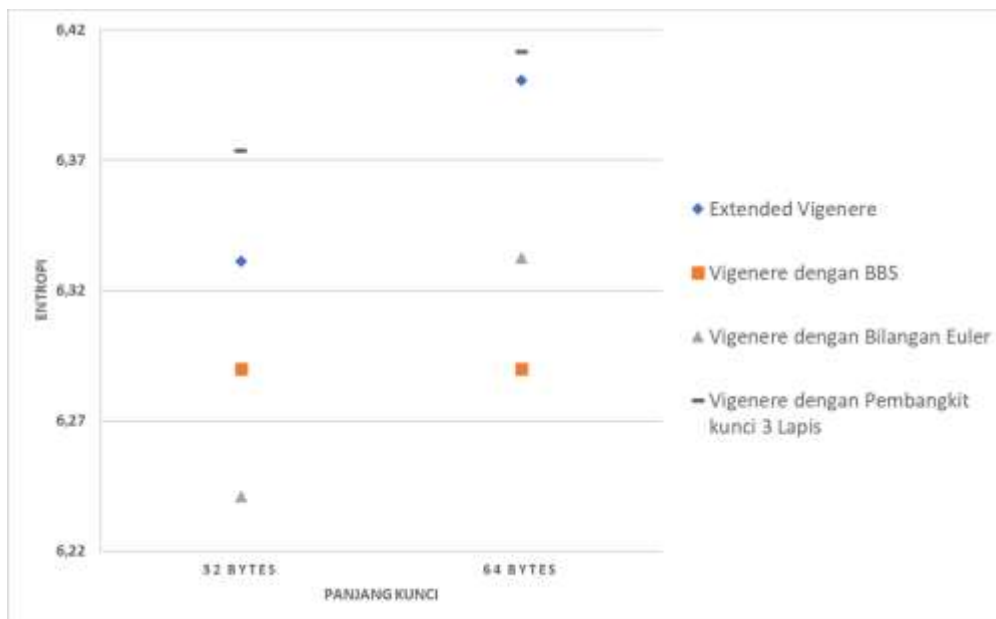
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T</						

adalah sampel yang sama yang digunakan pada eksperimen awal. Desain penerbitan kunci dilakukan secara sekuensial yang diawali dengan menggunakan fungsi random, bilangan Euler dan Blum Blum Shub. Penerbitan kunci menggunakan fungsi random dilakukan dengan memanfaatkan fungsi random yang terdapat pada (Nahar & Chakraborty, 2020). Hasil yang diperoleh digunakan sebagai input pada pembangkit kunci dengan bilangan euler. Pembangkit kunci bilangan euler mengadopsi dari pembangkit kunci yang dilakukan pada (Nofiyanto et al., 2017). Hasil yang diperoleh digunakan sebagai inputan pada pembangkit kunci Blum Blum Shub. Metode Blum Blum Shub mengadopsi dari (Telaumbanua & Zebua, 2020). Hasil akhir pada bagian penerbitan kunci ini ialah kunci yang digunakan pada proses enkripsi vigenere. Model enkripsi vigenere yang digunakan ialah extended vigenere (Nahar & Chakraborty, 2020). Tabel extended vigenere diperlihatkan pada gambar 4. Kunci yang digunakan terdapat 2 macam

yaitu kunci dengan panjang 32 Byte dan kunci dengan panjang 64 Byte. Cipherteks yang diperoleh selanjutnya dihitung nilai entropi sebagai metrik pengukuran capaian.

Hasil dan Pembahasan

Desain eksperimen pada gambar 3 diimplementasikan dengan mengadopsi penerbitan kunci vigenere tiga lapis. Sebagai sample digunakan informasi dari Astronomer Telegram Dataset dengan ukuran 1 KB. Sampel yang digunakan berformat teks dengan karakter ASCII. Proses yang dilakukan ialah sebagai berikut: Penerbit kunci fungsi random akan menghasilkan output yang digunakan sebagai input pada penerbit kunci bilangan Euler, output dari penerbit kunci bilangan Euler digunakan sebagai input pada penerbit kunci Blum Blum Shub, luarannya digunakan sebagai kunci pada proses enkripsi vigenere. Percobaan ini dilakukan dengan menghasilkan panjang kunci 32 Byte dan 64 Byte. Jumlah percobaan yang dilakukan sebanyak 50



Gambar 5 Perbandingan nilai entropi Extended Vigenere menggunakan pembangkit kunci berlapis dengan penelitian sebelumnya

kali dengan masing masing percobaan 25 kali untuk setiap kunci yang diterbitkan. Hasil yang diperoleh dihitung nilai entropi rata rata. Gambar 5 memperlihatkan grafik perbandingan vigenere dengan pembangkit kunci 3 lapis dengan metode sebelumnya.

Pembahasan

Gambar 5 memperlihatkan bahwa penggunaan pembangkit kunci secara berlapis pada vigenere memberikan nilai entropi yang lebih tinggi dibanding vigenere dengan pembangkit kunci lainnya. Dengan meningkatnya nilai entropi, maka metode pembangkit kunci secara berlapis mampu memberikan kewanaman yang lebih baik pada informasi. Nilai entropi rata rata yang diperoleh ialah 6,411717 pada panjang kunci 64 Byte dan 6,3736285 pada panjang kunci 32 Byte. Nilai entropi pada metode yang diusulkan adalah lebih baik dibanding nilai entropi pada metode sebelumnya yaitu 6,33126; 6,24114; 6,28985; 6,4007; 6,33272 dan 6,28985. Dengan peningkatan nilai entropi yang dihasilkan dari penggunaan penerit kunci secara berlapis, hal ini dapat diartikan bahwa informasi memiliki tingkat keamanan informasi yang lebih baik, dengan demikian informasi akan

lebih sulit untuk ditebak oleh kriptanalis. Tabel 1 memperlihatkan perbandingan nilai entropi yang diperoleh.

Tabel 2 memperlihatkan nilai capaian level keamanan informasi dalam bentuk prosentase (%) yang diperoleh pada eksperimen. Nilai entropi ideal ialah 8, ini berarti informasi yang diamankan dinilai sangat aman. Jika nilai entropi pada eksperimen dibandingkan dengan nilai entropi maksimal, maka akan didapatkan nilai capaian dalam bentuk prosentase. Nilai ini dapat dimaknai sebagai nilai capaian level keamanan informasi. Dengan capaian yang mendekati 100% maka dapat dianggap bahwa metode yang diusulkan memiliki tingkat keamanan yang lebih kuat sehingga produk cipherteks yang dihasilkan akan lebih sulit untuk ditebak. Peningkatan nilai entropi ini memberikan makna bahwa plainteks dan cipherteks semakin berbeda dan tidak memiliki hubungan yang berarti. Pada eksperimen yang dilakukan, diperoleh nilai capaian level keamanan informasi tertinggi ialah 80,15 %. Capaian 80% dalam vigenere dengan pembangkit kunci 3 lapis dengan panjang kunci 64 Byte, sedangkan capaian dengan kunci 32 Byte menunjukkan nilai

Tabel 1. Perbandingan Nilai Entropi

Panjang Kunci	Extended Vigenere	Vigenere dengan Bilangan Euler	Vigenere dengan Blum Blum Shub	Vigenere dengan Pembangkit Kunci 3 Lapis
32 Byte	6,33126	6,24114	6,28985	6,3736285
64 Byte	6,4007	6,33272	6,28985	6,411717

Tabel 2. Perbandingan Capaian Level Kewanaman Informasi

Panjang Kunci	Extended Vigenere (%)	Vigenere dengan Bilangan Euler (%)	Vigenere dengan Blum Blum Shub (%)	Vigenere dengan Pembangkit Kunci 3 Lapis (%)
32 Byte	79,14075	78,623125	78,01425	79,67035625
64 Byte	80,00875	78,623125	79,159	80,1464625

79,67 %. Hal ini dapat dikatakan bahwa panjang kunci akan mempengaruhi capaian tingkat keamanan yang lebih baik sehingga cipherteks yang dihasilkan akan semakin sulit ditebak oleh kriptanalis serta cipherteks memiliki ketidakterkaitan dengan plainteks yang lebih tinggi

Kesimpulan

Berdasarkan eksperimen yang dilakukan, maka dapat ditarik simpulan bahwa penggunaan penggunaan penerbitan kunci secara berlapis pada model enkripsi vigenere mampu meningkatkan tingkat keamanan informasi. Dengan demikian informasi akan semakin sulit ditebak dan dipecahkan. Aspek lain yang diperoleh ialah bahwa penggunaan panjang kunci juga memiliki pengaruh dalam peningkatan level keamanan informasi. Dengan demikian penerbitan kunci dalam model enkripsi vigenere adalah sebagai penentu dalam confidentiality informasi.

Daftar Pustaka

- B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *Journal of the Operations Research Society of China*, 2020, doi: 10.1007/s40305-020-00320-x
- H. Rahmah Zagi Asst Abeer Tariq Maalood, "A New Key Generation to Greate Enhanced Security Version of AES Encryption Method," *Journal of College of Education*, no. 2, pp. 1–16, 2021.
- J. Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *International Journal of Information System & Technology Akreditasi*, vol. 4, no. 1, pp. 471–481, 2020.
- K. Nahar and P. Chakraborty, "A Modified Version of Vigenere Cipher using 95×95 Table," *International Journal of Engineering & Advanced Technology (IJEAT)*, vol. 9, no. 5, pp. 1144–1148,

- 2020, doi: 10.35940/ijeat.E9941.069520.
- R. R. Fauzi and W. Theophilus, "Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice," *AITI: Jurnal Teknologi Informasi*, vol. 18, no. Agustus, pp. 158–172, 2021.
- E. Ardianto, W. T. Handoko, E. Supriyanto, and H. Murti, "Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi," *JURNAL INFORMATIKA UPGRIS*, vol. 7, no. 2, pp. 23–27, 2021.
- S. Park, J. Kim, K. Cho, and D. H. Yum, "Finding the key length of a Vigenère cipher: How to improve the twist algorithm," *Cryptologia*, vol. 44, no. 3, pp. 197–204, May 2020, doi: 10.1080/01611194.2019.1657202.
- A. P. Sidik, "Improve The Security of The Vigenère Cypher Algorithm by Modifying the Encoding Table and Key," *International Journal of Basic and Applied Science*, vol. 10, no. 2, pp. 42–50, 2021, [Online]. Available: www.ijobas.pelnu.ac.id
- N. Uniyal, G. Dobhal, A. Rawat, and A. Sikander, "A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication," *Wireless Personal Communications*, vol. 119, no. 2, pp. 1577–1587, Jul. 2021, doi: 10.1007/s11277-021-08295-5
- N. Nofiyanto, hamzah Hamzah, and H. Surbakti, "Short Message Encryption Application Development Using Vigenere Algorithm Utilizing Euler's Number On Android Smartphone," *Jurnal Teknologi Informasi*, vol. 9, no. 27, pp. 81–92, 2014.
- F. Telaumbanua and T. Zebua, "Modifikasi Vigenere Cipher Dengan Pembangkit Kunci Blum Blum Shub," *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 4, no. 1, 2020, doi: 10.30865/komik.v4i1.2646
- A. Susanto *et al.*, "Triple layer image security using bit-shift, chaos, and stream encryption," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 980–987, Jun. 2020, doi: 10.11591/eei.v9i3.2001
- Z. Qowi and N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," in *Journal of Physics:*

- Conference Series*, Jun. 2021, vol. 1918, no. 4, pp. 1–6. doi: 10.1088/1742-6596/1918/4/042009
- F. Telaumbanua and T. Zebua, “Modifikasi Vigenere Cipher Dengan Pembangkit Kunci Blum Blum Shub,” *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 4, no. 1, 2020, doi: 10.30865/komik.v4i1.2646.
- K. Nahar and P. Chakraborty, “A Modified Version of Vigenere Cipher using 95×95 Table,” *International Journal of Engineering & Advanced Technology (IJEAT)*, vol. 9, no. 5, pp. 1144–1148, 2020, doi: 10.35940/ijeat.E9941.069520.
- H. Surbakti, “Short Message Encryption Application Development Using Vigenere Algorithm Utilizing Euler’s Number On Android Smartphone,” *Jurnal Teknologi Informasi*, vol. 9, no. 27, pp. 81–92, 2014.
- Ahamed, B. B., & Krishnamoorthy, M. (2020). SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm. *Journal of the Operations Research Society of China*. <https://doi.org/10.1007/s40305-020-00320-x>
- Ardhianto, E., Handoko, W. T., Supriyanto, E., & Murti, D. H. (2021). Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi. *JURNAL INFORMATIKA UPGRIS*, 7(2).
- Fauzi, R. R., & Theophilus, W. (2021). Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice. *AITI: Jurnal Teknologi Informasi*, 18(Agustus), 158–172.
- Nahar, K., & Chakraborty, P. (2020). A Modified Version of Vigenere Cipher using 95 95 Table. *International Journal of Engineering and Advanced Technology*, 9(5), 1144–1148. <https://doi.org/10.35940/ijeat.E9941.069520>
- Nofiyanto, N., Hamzah, H., & Surbakti, H. (2017). Short Message Encryption Application Development Using Vigenere Algorithm Utilizing Euler’s Number On Android Smartphone. *Respati*, 9(27). <https://doi.org/10.35842/jtir.v9i27.85>
- Park, S., Kim, J., Cho, K., & Yum, D. H. (2020). Finding the key length of a Vigenère cipher: How to improve the twist algorithm. *Cryptologia*, 44(3), 197–204. <https://doi.org/10.1080/01611194.2019.1657202>
- Politeknik Ganesha Medan, R. (2020). Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security. *International Journal of Information System & Technology Akreditasi*, 4(1), 471–481.
- Purnomo Sidik, A. (2021). Improve The Security of The Vigenère Cypher Algorithm by Modifying the Encoding Table and Key. *International Journal of Basic and Applied Science*, 10(2), 42–50. <https://doi.org/10.35335/ijobas.v10i2.54>
- Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, 1918(4), 042009. <https://doi.org/10.1088/1742-6596/1918/4/042009>
- Rahmah Zagi Asst Abeer Tariq Maalood, H. (2021). A New Key Generation to Greater Enhanced Security Version of AES Encryption Method. *Journal of College of Education*, 2.
- Susanto, A., Setiadi, D. R. I. M., Rachmawanto, E. H., Wahyu Mulyono, I. U., Sari, C. A., Sarker, M. K., & Sazal, M. R. (2020). Triple layer image security using bit-shift, chaos, and stream encryption. *Bulletin of Electrical Engineering and Informatics*, 9(3), 980–987. <https://doi.org/10.11591/eei.v9i3.2001>
- Telaumbanua, F., & Zebua, T. (2020). Modifikasi Vigenere Cipher Dengan Pembangkit Kunci Blum Blum Shub. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, 4(1). <https://doi.org/10.30865/komik.v4i1.2646>

Uniyal, N., Dobhal, G., Rawat, A., & Sikander, A. (2021). A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication. *Wireless*

Personal Communications, 119(2), 1577–1587.
<https://doi.org/10.1007/s11277-021-08295-5>