GENERATOR KUNCI TIGA LAPIS PADA ALGORITMA VIGENERE MENGGUNAKAN FUNGSI RANDOM, BILANGAN EULER DAN METODE BLUM BLUM SHUB

[1]Sutrasno Andre Wibowo,[2]Eka Ardhianto
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank
[1,2]Jl. Tri Loma Juang No. 1, Semarang, Jawa Tengah
[1]andresutrasno381@gmail.com, [2]ekaardhianto@edu.unisbank.ac.id

Abstrak

Keamanan informasi melalui jaringan menjadi pokok penting dalam berkomunikasi. Meskipun model informasi yang berkembang saat ini beragam, model komunikasi berbasis teks masih banyak digunakan seperti surat elektronik, pesan singkat, telegram dan aplikasi yang serupa. Algoritma Vigenere yang berbasis teks hingga sekarang masih dikembangkan untuk membantu pengamanan informasi. Evolusi vigenere dimotivasi untuk meningkatkan keamanan informasi. Salah satu faktor yang penting dalam vigenere untuk meingkatkan tingkat keamanan informasi ialah kunci yang digunakan, oleh karena itu pemilihan kunci yang tepat akan mampu meningkatkan ketahanan informasi. Penelitian ini bertujuan untuk meningkatkan ketahanan Algoritma Vigenere terhadap serangan kriptanalis dengan menggunakan penerbitan kunci secara berlapis. Metode yang digunakan untuk menerbitkan kunci ialah kombinasi dari fungsi random, bilangan euler dan metode blum blum shub yang diimplementasikan pada model enkripsi extended vigenere. Entropi digunakan sebagai metric performa dari setiap model yang dieksperimenkan. Dengan eksperimen yang dilakukan secara berulang dengan sampel yang sama, hasil yang diperoleh ialah capaian nilai entropi rata-rata dengan nilai lebih dari 80% dari entropi optimum pada nilai entropi 6,41 dibanding dengan pengembangan model enkripsi vigenere sebelumnya. Dengan demikian modifikasi algoritma vigenere yang diusulkan memiliki ketahanan yang lebih baik terhadap serangan kriptanalis dari versi sebelumnya.

***Kata Kunci**: Entropi, Informasi, Kunci, Vigenere.*

Abstract

Information security over the network is an important point in communication. Although the information models that are currently developing are various, text-based communication models are still widely used such as electronic mail, short messages, telegrams and similar applications. The text-based Vigenere algorithm is still being developed to help secure information. The evolution of vigenere is motivated to improve information security. One of the important factors in vigenere to increase the level of information security is the key used, therefore choosing the right key will be able to increase information security. This study aims to increase the resilience of the Vigenere Algorithm against cryptanalytic attacks by using layered key issuance. The method used to issue the key is a combination of random functions, euler numbers and the blum blum shub method which is implemented in the extended vigenere encryption model. Entropy is used as a performance metric of each experimental model. With repeated experiments with the same sample, the results obtained are the achievement of the average entropy value with a value of more than 80% of the optimum entropy at an entropy value of 6.41 compared to the previous development of the Vigenere encryption model. Thus the

proposed vigenere algorithm modification has better resistance to cryptanalyst attacks than the previous version

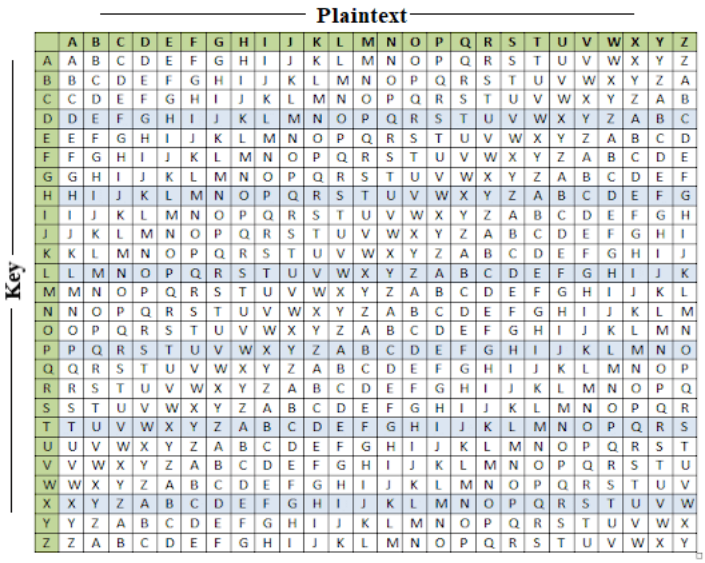
***Keywords**: Entropy, Information, Key, Vigenere.*

PENDAHULUAN

Salah satu kegiatan utama dalam komunikasi dunia digital ialah berbagi informasi. Informasi yang dibagikan dapat berupa teks, suara dan gambar dalam format digital dalam percakapan publik, pribadi atau komunikasi dalam bentuk lain [1]. Penyampaian informasi secara pribadi melalui jaringan internet yang terbuka tentunya akan terdapat batasan entias yang dapat mengakses informasi tersebut, oleh karena itu sangat penting untuk mengirim informasi yang rahasia secara aman. Aspek penting dalam menjaga keamanan informasi dikenal sebagai *confidentiality*. *Confidentiality* pada bidang informasi dapat dicapai dengan cara menyandikan informasi menggunakan teknik kriptografi [2]. Tujuan utama kriptografi ialah untuk menjaga kerahasiaan informasi[3]. 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 [1]. Plainteks ialah informasi yang menggunakan bahasa normal untuk komunikasi, sedangkan cipherteks ialah pesan yang sudah menjadi teks sandi [4]. Enkripsi ialah proses mengatur ulang pesan asli ke dalam format yang tidak dapat dikenali [5] dengan pengertian lain mengubah data asli (plaintext) menjadi data samar (ciphertext) yang telah teracak sedemikian rupa hingga sulit dimengerti oleh pihak lain [5], sedangkan cara untuk mendapatkan kembali pesan sebelumnya disebut sebagai dekripsi[4] dengan pengetian lain proses yang mengubah kembali data samar (ciphertext) menjadi data asli (plaintext) [5].

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[6]. 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*)[7]. Vigenere memiliki sifat kriptografi simetris, yaitu menggunakan kunci yang sama pada proses enkripsi dan dekripsinya [6], [8]. 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. 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 [9]. Penggunaan kunci vigenere yang pendek dan berulang akan menyebabkan kerentanan dalam pengamanan informasi [6]. Modifikasi kunci pada vigenere salah satunya ialah penggunaan *Euler Number* [10]. Bilangan Euler diadopsi dalam vigenere cipher memberikan keacakan dalam merahasiakan informasi, sehingga menyulitkan kriptanalis. Modifikasi kunci lainnya ialah penggunaan pembangkit kunci Blum Blum Shub [11]. 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 [11]. Modifikasi vigenere juga dilakukan dengan memperbanyak karakter set menjadi 96 simbol. Modifikasi ini dikenal sebagai *Extended Vigenere*. Modifikasi ini menghasilkan bentuk tabel vigenere dengan ukuruan 95x95, lebih besar dibanding vigenere yang asli menggunakan jumlah alfabet 26x26. Modifikasi ini dilakukan dengan tujuan untuk meningkatkan keamanan informasi dan mempersulit kriptanalis [4]. 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.

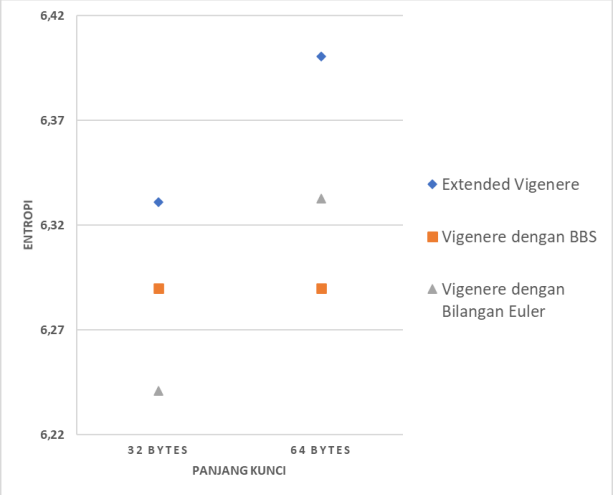


Gambar 1. Tabel Vigenere Cipher
[sumber: [6]]

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 [12]. 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.

$$E = -\sum_{r=0}^{R=255} c(r) log_2(c(r)) \quad (1)$$

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.



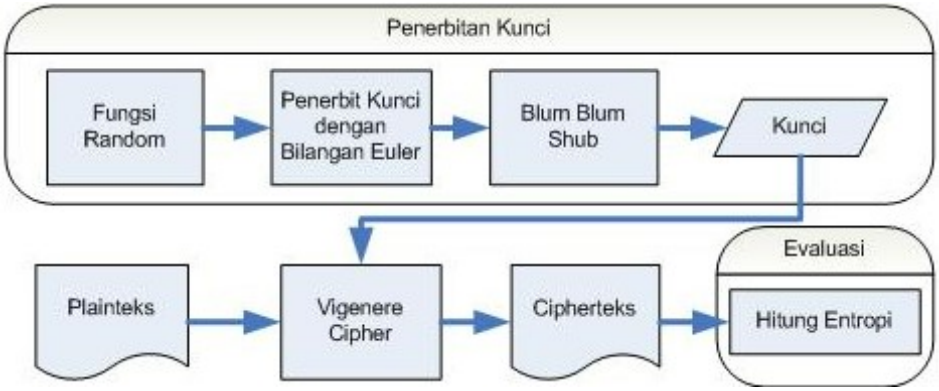
Gambar 2. Nilai Entropi Cipherteks Vigenere Cipher pada Eksperimen Awal
[diadopsi dari : [4], [10], [11]]

Penggunaan kunci pada vigenere merupakan hal yang paling krusial. Kunci vigenere secara umum adalah pendek dan digunakan secara berulang [13]. Penggunaan kunci yang dipilih secara manual juga akan menjadikan kerapuhan dalam vigenere. Selain itu permasalahan distribusi kunci simetris ini akan menimbulkan kecurigaan [8]. 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 meningkatkan ketahanan Algoritma Vigenere terhadap serangan kriptanalis dengan menggunakan 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 vigenere dan diukur nilai entropi cipherteksnya.

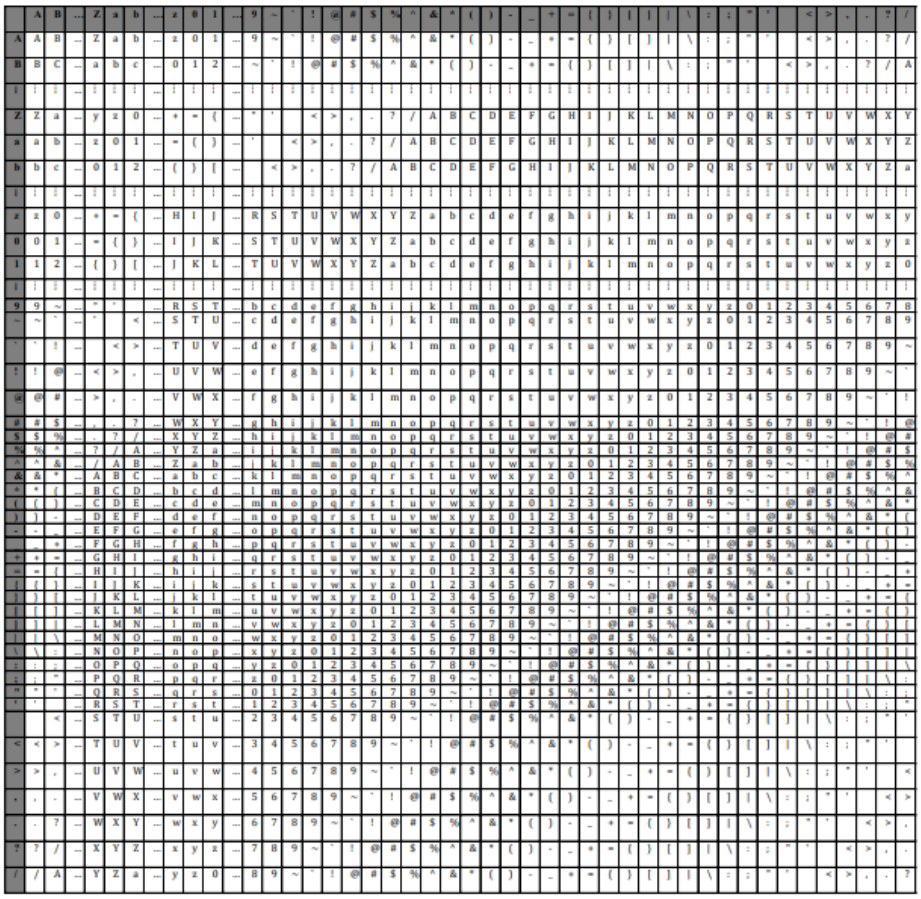
METODE PENELITIAN

Eksperimen pengembangan 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 modifikasi penerbitan kunci pada extended vigenere. Penelitian ini melakukan eksperimen awal dan eksperimen pengembangan. Eksperimen awal dilakukan untuk melihat performa algoritma vigenere yang telah dikembangkan [14]–[16] sebagai state-of the art. Nilai yang diperoleh seperti pada gambar 2 digunakan sebagai pembanding pada nilai eksperimen pengembangan. Eksperimen pengembangan dilakukan dengan memodifikasi penerbitan kunci pada vigenere secara berlapis. Eksperimen pengembangan menggunakan sampel plainteks dari Astronomer Telegram Dataset dengan ukuran 1 KB. Sampel ini adalah sampel yang sama yang digunakan pada eksperiemen 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 [15]. Hasil yang diperoleh digunakan sebagai input pada pembangkit kunci dengan bilangan euler. Pembangkit kunci bilangan euler mengadopsi dari pembangkit kunci yang dilakukan pada [16]. Hasil yang diperoleh digunakan sebagai inputan pada pembangkit kunci Blum Blum Shub. Metode Blum Blum Shub mengadopsi dari [14]. Hasil akhir pada bagian penerbitan kunci ini ialah kunci yang digunakan pada proses enkripsi vigenere. Model enkripsi vigenere yang digunakan ialah extended vigenere [15]. 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.



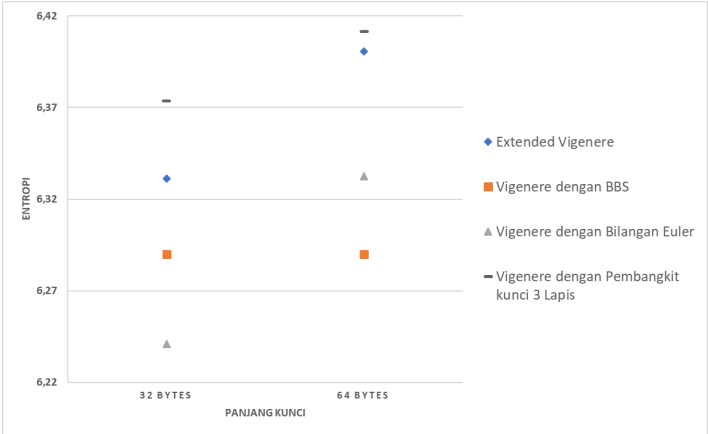
Gambar 3. Desain Modifikasi Penerbitan Kunci pada Extended Vigenere



Gambar 4. Tabel Extended Vigenere
[diadopsi dari [15]]

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 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. Gambar 5 memperlihatkan bahwa penggunaan pembangkit kunci secara berlapis pada vigenere memberikan nilai entropi yang lebih tinggi dibanding vigenere dengan pembangkit kunci lainnnya. Dengan meningkatnya nilai entropi, maka metode pembangkit kunci secara berlapis mampu memberikan kemanan 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.



Gambar 5. Perbandingan Nilai Entropi Extended Vigenere, Vigenere dengan Bilangan Euler, Vigenere dengan Blum Blum Shub (BBS) dan Vigenere dengan Pembangkit Kunci 3 Lapis

.

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 Kemanan Informasi

Panjang Kunci	Extended Vigenère (%)	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

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 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 DAN SARAN

Berdasarkan ekperimen yang dilakukan, maka dapat ditarik simpulan bahwa penggunaan penerbitan kunci secara berlapis pada model enkripsi vigenere mampu meningkatkan ketahanan Algoritma Vigenere dari serangan kriptanalis.

Dengan peningkatan nilai entropi yang diperoleh maka informasi atau pesan yang dienkripsi akan semakin acak sehingga akan semakin sulit ditebak dan dipecahkan. Aspek lain yang menjadi perhatian dalam eksperimen ini ialah bahwa penggunaan panjang kunci juga memiliki pengaruh dalam peningkatan

level keamanan informasi. Dengan demikian desain penerbitan kunci dalam model enkripsi vigenere adalah sebagai penentu dalam *confidentiality* informasi.

Meskipun temuan dalam eksperimen ini Vigenere menjadi lebih baik dari versi sebelumnya, namun eksperimen ini masih terbatas pada bentuk informasi berbasis teks. Sebagai bahan pertimbangan kelanjutan riset perlu pengembangan dengan menggunakan bentuk informasi berbasis piksel, suara, gelombang radio serta melakukan kombinasi dengan algoritma lain untuk pencapaian keamanan informasi maksimal.

DAFTAR PUSTAKA

[1] 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.

[2] H. Rahmah Zagi Asst Abeer Tariq Maolood, "A New Key Generation to Greate Enhanced Security Version of AES Encryption Method," *Journal of College of Education*, no. 2, pp. 1–16, 2021.

[3] 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.

[4] 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.

[5] 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.

[6] E. Ardhianto, 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.

[7] 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.

[8] 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.pelnus.ac.id

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.