

# Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi

**E. Ardianto<sup>1</sup>, W. T. Handoko<sup>2</sup>, E. Supriyanto<sup>3</sup> dan H. Murti<sup>4</sup>**

<sup>1,2</sup>Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Stikubank Semarang

<sup>3</sup>Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Stikubank Semarang

Jl. Tri Lomba Juang No. 1, Semarang

E-mail : ekaardhianto@edu.unisbank.ac.id<sup>1</sup>, wthandoko@edu.unisbank.ac.id<sup>2</sup>, edysupriyanto@edu.unisbank.ac.id<sup>3</sup>, harimurti@edu.unisbank.ac.id<sup>4</sup>

*Abstract—The information exchange through the public sphere still leaves vulnerabilities, so it needs security through a cryptographic process. One of the cryptographic models that can stand for more than 300 years called Vigenere Cipher, before being solved by Kasiski and Friedman. This article discusses the development and evolution of the Vigenere Cipher. Until now, the use of Vigenere Cipher can still be applied to make information exchange and communication transactions. Its development, the Vigenere evolution focuses on three parts, the development by the hybrid method, the development by the key generating process and the development by the number of character sets in Vigenere. Based the development of these three focuses, Vigenere Cipher has ability to provide a better level of security for the encoded information. Another advantage is that the Vigenere Cipher with this development can be applied and accepted for security and information exchange in a wider field.*

*Abstrak—Pertukaran informasi melalui ruang publik masih menyisakan kerentanan keamanan, sehingga perlu mekanisme pengamanan melalui proses kriptografi. Salah satu model kriptografi yang dapat bertahan hingga lebih dari 300 tahun adalah Vigenere Cipher, sebelum dipecahkan oleh Kasiski dan Friedman. Artikel ini membahas tentang perkembangan dan evolusi Vigenere Cipher. Hingga saat ini, penggunaan Vigenere Cipher masih dapat diaplikasikan untuk mengamankan petukaran informasi dan transaksi komunikasi. Dalam perkembangannya, bentuk evolusi pada Vigenere terfokus pada tiga bagian, pengembangan dengan metode hibrid, pengembangan pada proses penerbitan kunci yang digunakan dan pengembangan pada jumlah karakter set yang digunakan pada Vigenere. Dengan pengembangan pada ketiga fokus tersebut, maka Vigenere Cipher mampu menyuguhkan tingkat keamanan yang lebih baik pada informasi yang disandikannya. Keuntungan lain adalah Vigenere Cipher dengan pengembangan ini dapat diaplikasikan dan diterima untuk pengamanan dan pertukaran informasi pada bidang yang lebih luas.*

*Kata Kunci—Vigenere, Cipher, Informasi, Kunci, Pengembangan .*

## I. PENDAHULUAN

Komunikasi internet antara dua entitas atau lebih memiliki tujuan untuk menyampaikan informasi. Informasi yang disampaikan dapat berupa teks, gambar, file, pesan publik serta bentuk bentuk percakapan [1]. Bentuk informasi yang disampaikan juga dapat berupa informasi rahasia. Penggunaan internet saat ini telah menjadi selayaknya kebutuhan publik yang luas dan sangat terbuka. Kebocoran informasi rahasia dalam internet mungkin akan dapat terjadi, sehingga diperlukan sebuah mekanisme pengamanan yang cukup tangguh untuk menjaganya.

Metode terbaik yang dapat digunakan untuk mengamankan informasi adalah dengan cara mensandikannya. Untuk mensandikan informasi, teknik kriptografi merupakan teknik pengamanan informasi yang paling cepat berkembang. Kriptografi merupakan sebuah cara untuk mengamankan sebuah informasi asli yang disusun acak dan tidak dapat dipahami selain entitas yang berhak menerimanya [2].

Salah satu model kriptografi yang cukup bertahan lama adalah algoritma Vigenere atau dikenal sebagai Vigenere Cipher. Vigenere Cipher dipublikasikan pada tahun 1586 oleh Blaise de Vigenere yang pada saat itu digunakan untuk memproses pengamanan informasi dalam bentuk teks [3]. Vigenere digolongkan pada algoritma kriptografi kunci

simetris, hal ini karena penggunaan kunci pada proses enkripsi dan dekripsi adalah sama [1] [4]. Vigenere memproses informasi dalam bentuk teks antara teks informasi pesan dan teks kata kunci, sehingga vigenere juga dikategorikan sebagai polyalphabetic cipher [1]. Kunci dalam Vigenere digunakan secara berulang sebanyak jumlah teks informasi yang akan disandikan [3]. Proses pada Vigenere Cipher digambarkan seperti proses Caesar Cipher dengan nilai pergeseran karakter yang berbeda seperti terlihat pada gambar 1. Dengan jumlah karakter set yang standar, gambar 2 menunjukkan alur proses pembuatan informasi rahasia menggunakan Vigenere Cipher. Vigenere Cipher merupakan salah satu model pengamanan informasi yang kuat pada masanya, hingga pada tahun 1917 dapat dipecahkan oleh Friedman dan Kasiski [5]. Untuk itu pengembangan dan modifikasi pada Vigenere Cipher sangat mungkin untuk dilakukan dalam tujuan memperkuat dan menutup celah keamanan pada informasi yang dirahasiakan.

Bentuk perkembangan sebuah algoritma dapat dianggap sebagai sebuah evolusi algoritma tersebut. Dalam mengembangkan sebuah algoritma dan metode, perlu adanya sebuah penelusuran yang cukup supaya terdapat alur pengembangan yang jelas dan lebih terukur. Artikel ini akan mengulas perkembangan Vigenere Cipher dengan mengadopsi proses tinjauan sistematis literatur, serta

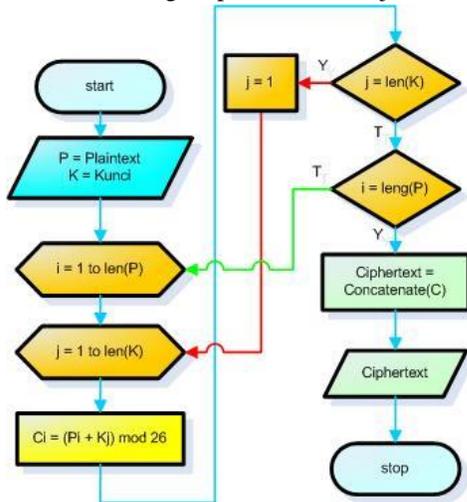
masuk - masuk untuk pengembangan lebih lanjut terhadap Vigenere Cipher dengan beberapa kemungkinan pendekatan.

II. METODE PENELITIAN

Studi empiris dibidang ilmu komputer saat ini lebih sering digunakan untuk melihat fenomena yang ada. Penelusuran

Gambar. 1. Tabel Vigenere. Diadopsi dari [4].

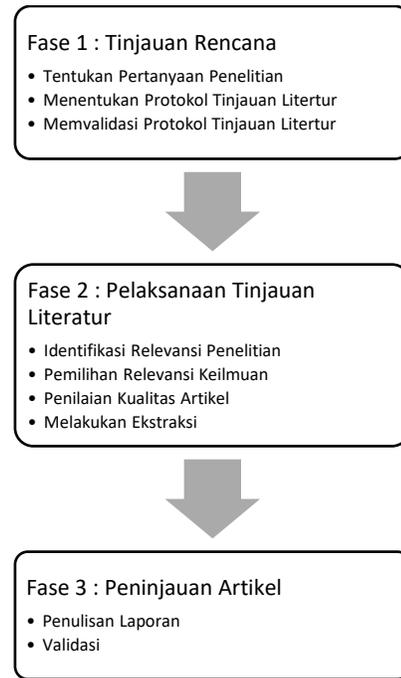
dalam artikel ini mengadopsi teknik Tinjauan Literatur



Gambar. 2. Alur Proses Enkripsi Vigenere Cipher. Diadopsi dari [4].

Sistematis seperti pada [6] [7]. Proses tinjauan ditunjukkan pada gambar 3. Tinjauan Literatur Sistematis bertujuan untuk memberikan tinjauan komprehensif literatur terkini yang relevan dengan beberapa rumusan masalah. Beberapa artikel di bidang rekayasa ilmu komputer mengadopsi [6] untuk melakukan tinjauan literatur sistematis.

Proses Tinjauan Literatur terdiri dari tiga fase dengan sembilan aktivitas. Pada fase pertama, sebagai pertanyaan penelitian 1 (RQ1) ialah apakah algoritma vigenere masih dikembangkan hingga saat ini? Dan sebagai pertanyaan penelitian 2 (RQ2) ialah tentang bagaimana bentuk evolusi pada algoritma vigenere?. Pertanyaan penelitian ini ditentukan pada fase awal sebelum melakukan tahap lebih lanjut.



Gambar. 3. Alur Proses Tinjauan Literatur. Diadopsi dari [6].

Protokol peninjauan literatur mencakup sumber yang akan digunakan, periode waktu artikel yang akan ditinjau, kata kunci yang digunakan. Protokol tinjauan literatur ditunjukkan pada tabel 1. Sumber yang digunakan adalah artikel penelitian yang terindeks pada Google Cendikia yang terbit pada tahun 2017 hingga 2021. Hal ini dipandang karena bentuk pengembangan lebih lanjut akan menemukan pengembangan terkini dari artikel yang didapatkan. Artikel yang akan ditinjau adalah artikel yang diterbitkan pada Jurnal dan Prosiding.

Pengumpulan artikel didasarkan pada kata kunci pencarian pada Tabel 1 yang bersesuaian dengan kata kunci dan abstrak artikel yang dapat diunduh. Kriteria kualitas yang ditetapkan untuk menilai studi adalah mengklasifikasikan makalah dalam ulasan jika berisi model, eksperimen atau kerangka kerja. Data yang diperlukan diekstraksi dari artikel yang didapatkan untuk menjawab pertanyaan penelitian yang diajukan.

Langkah lain yang dilakukan dalam proses pencarian adalah mencari pada area kerja terkait dari artikel yang dipilih untuk meningkatkan kekuatan ulasan dengan mengonfirmasi bahwa tidak ada referensi berharga yang terlewatkan selama proses literasi. Data yang dikumpulkan disintesis untuk menunjukkan hasil yang lengkap. Pada fase

Tabel 1. Protokol Tinjauan Literatur

Tahun Terbit Artikel	Sumber	Kata Kunci Pencarian
2017 – 2021	Google Cendikia	vigenere algorithm modification

ketiga dari proses Tinjauan Literatur adalah menuliskan laporan dan memvalidasi.

III. HASIL DAN PEMBAHASAN

Tinjauan literatur yang dilakukan dengan kata kunci pencarian mendapatkan hasil sebanyak 916 artikel yang ditampilkan oleh sumber. Dengan batasan tahun penerbitan artikel, di dapatkan 29 artikel yang relevan dengan pertanyaan penelitian. Tabel 2 menunjukkan distribusi artikel pertahun yang didapatkan pada tinjauan literatur. Dan Tabel 3 menunjukkan jenis artikel jurnal dan artikel prosiding. Dengan adanya artikel yang masih di dapatkan dalam proses penelusuran literatur, maka Vigenere Cipher masih dikembangkan hingga sekarang.

Dari artikel yang diperoleh, pengembangan yang dilakukan pada Vigenere Cipher adalah untuk menutup celah kelemahan dan meningkatkan keamanan informasi yang disandikan. Dari proses ekstraksi data dari artikel yang diperoleh, bentuk pengembangan pada Vigenere Cipher dikelompokkan menjadi tiga, kelompok pertama adalah pengembangan dengan mengkombinasi Vigenere Cipher dengan algoritma lain. pengembangan Vigenere Cipher

Tabel 2.  
Tahun Publikasi Artikel

TAHUN PENERBITAN	JUMLAH ARTIKEL
2017	4
2018	7
2019	8
2020	9
2021	1

Tabel 3.  
Jenis Artikel

JENIS	JUMLAH ARTIKEL
Artikel Jurnal	16
Artikel Prosiding	13

dengan cara ini sebanyak 13 artikel. Kedua adalah dengan memodifikasi cara penerbitan kunci pada Vigenere Cipher. Pada cara ini terdapat 15 artikel yang membahasnya. Ketiga adalah dengan memperluas penggunaan karakter set yang digunakan pada Vigenere Cipher, terdapat 5 artikel yang mengulasnya. Bentuk pengelompokan artikel yang melakukan pengembangan pada Vigenere Cipher dapat dilihat pada tabel 4.

A. Pengembangan Dengan Hybrid Method

Pengembangan Vigenere Cipher tentunya difokuskan pada bagaimana menaikkan tingkat keamanan dari informasi yang disandikan. Penggabungan Vigenere Cipher dengan algoritma lain, dipandang sebagai sebuah solusi untuk menutup celah kelemahannya. Meningkatkan keamanan dengan menggabungkan Vigenere dan Stream Cipher dinilai memiliki keamanan yang tinggi disbanding pengamanan informs hanya menggunakan Vigenere saja [8]. Hal ini juga dipandang akan menyuliskan kriptanalisis untuk memecahkan informasi yang disandikan. Model peningkatan lainnya adalah menggabungkan Vigenere dengan Hill Cipher. Semakin banyak proses enkripsi yang

Tabel 4.  
Kategori Pengembangan Vigenere Cipher

No	Indeks Artikel	Mengkombinasi dengan Algoritma Lain	Memodifikasi Cara Penerbitan Kunci	Memperluas Penggunaan Karakter Set
1	[1]	-	Y	-
2	[2]	-	-	Y
3	[3]	Y	Y	-
4	[4]	-	-	Y
5	[5]	-	Y	-
6	[14]	Y	-	-
7	[27]	-	-	Y
8	[18]	-	Y	-
9	[29]	-	Y	-
10	[26]	-	-	Y
11	[30]	Y	-	-
12	[15]	Y	Y	-
13	[13]	Y	Y	-
14	[19]	-	Y	-
15	[31]	-	Y	-
16	[21]	-	Y	-
17	[16]	Y	-	-
18	[8]	Y	-	-
19	[22]	-	Y	-
20	[24]	-	Y	-
21	[23]	-	Y	-
22	[25]	-	Y	-
23	[9]	Y	-	-
24	[17]	Y	-	-
25	[20]	-	Y	-
26	[11]	Y	-	-
27	[10]	Y	-	-
28	[12]	Y	-	-
29	[28]	Y	-	Y

dilakukan maka akan semakin lama waktu untuk memecahkan informasi asli yang disandikan, artinya semakin aman untuk merahasiakan informasi [9]. Hibridisasi Vigenere dengan Hill Cipher juga dilakukan dengan memandang ukuran kunci pada Vigenere yang dinilai terlalu kecil sehingga akan rentan dengan model serangan secara statistic, bentuk kelemahan lain adalah adanya penempatan dua karakter yang sama pada blok yang berbeda. Dengan mengkohesikan dua model ini maka akan terbentuk algoritma yang lebih handal [10]. Peningkatan level keamanan lain adalah pada objek citra, yakni menggabungkan Vigenere menggunakan bitswap dan transposisi acak [11]. Hasil kinerja yang didapatkan ialah bahwa Entropi tertinggi diperoleh dari VC yang dioptimasi dengan bitswap dan transposisi acak yaitu nilai entropi rata-rata sebesar 7.9582. Peningkatan rata-rata entropi ini adalah sebesar 37% dibanding entropi citra aslinya. Koefisien korelasi hasil enkripsi rata-rata adalah sebesar 0.0195. Artikel lain menyatakan bahwa perbaikan tingkat keamanan dapat dilakukan dengan melakukan praenkripsi, yakni melakukan perubahan bentuk karakter plainteks dengan menggunakan teknik flip and shift kolom [12]. Modifikasi ini menghasilkan nilai korelasi yang lebih baik dibandingkan proses pengamanan dengan Vigenere saja. Modifikasi Vigenere untuk menjadi sebuah Super Enkripsi dilakukan juga dengan menggabungkan kriptografi One Time Pad [3] [13]. Hasil kombinasinya selain menaikkan kemanan informasi juga akan mempercepat waktu penyandian informasi.

Penggabungan Vigenere Cipher dalam ranah steganografi untuk mengamankan informasi juga dilakukan. Teknik gabungan antara Caesar-Vigenere digabungkan dengan teknik Steganografi Last Significant Bit (LSB) untuk mengamankan dan menyembunyikan informasi kedalam sebuah media gambar [14]. Vigenere juga digabungkan dengan AES untuk pengamanan informasinya, serta teknik penyembunyian LSB ditambahkan untuk menyembunyikan informasi tersandi pada media gambar [15]. Pada teknik ini, pertukaran kunci antara pengirim dan penerima menggunakan teknik Diffie-Helman. Media audio juga digunakan sebagai tempat penyembunyian informasi yang disandikan dengan Vigenere, teknik LSB digunakan untuk penyematannya [16]. Pengembangan Vigenere dengan teknik Steganografi akan memperkuat pengamanan substansi informasi rahasia melalui penyamaran informasi sehingga akan lebih sulit teridentifikasi [17].

### B. Pengembangan dengan Modifikasi Kunci

Pengamanan informasi menggunakan Vigenere juga dikembangkan dengan memodifikasi penerbitan kunci yang digunakan. Vigenere Cipher standar menggunakan kunci pendek yang diulang, hal ini dipandang sebagai celah kerapuhan Vigenere. Penggunaan Euler Nuber sebagai pembangkit kunci diusulkan untuk menambah kekuatan Vigenere supaya tahan terhadap serangan kriptanalis [18]. Hasil yang didapat ialah bahwa bentuk kunci yang diterbitkan dengan menggunakan Euler Number menjadi acak dan panjang. Memodifikasi Vigenere untuk meningkatkan kecepatan enkripsi dan dekripsi melalui teknik pembangkitan kunci yang sederhana namun cepat menggunakan operasi bitwise XBOX dan XOR juga diupayakan [19]. Teknik pembuatan kunci mencakup pemetaan (XBOX dan XOR) untuk meningkatkan keamanannya. Hasilnya menunjukkan bahwa algoritma yang dimodifikasi berkinerja lebih baik dan telah meningkatkan kecepatan enkripsi dan dekripsinya. Proses pembangkitan kunci lainnya dilakukan berdasarkan pembangkit kunci blum blum shub, artinya kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang dibangkitkan berdasarkan pembangkit kunci blum blum shub, sehingga proses modifikasi yang dilakukan dalam pembangkitan kunci tersebut dapat meminimalkan tindakan pemecahan kunci yang dilakukan pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan data [20]. Penggunaan kunci pada RSA dimanfaatkan sebagai penerbit kunci pada Vigenere [1]. RSA terkenal keamanannya dengan model kunci asimetrisnya namun memakan waktu proses yang cukup lama, dengan menggabungkan Vigenere dan RSA pada pembangkitan kunci maka informasi yang disandikan akan lebih aman dan membutuhkan waktu proses yang relative lebih singkat dari pada RSA. Penerbitan kunci juga diusulkan dengan menggunakan tabel distribusi yang disusun secara acak dan dinamis dengan melihat panjang karakter informasi yang disandikan [21]. Ekspansi kunci pada Vigenere juga mengadopsi pembangkitan kunci pada Rivest Code 6 (RC6)

[5] [22]. Bentuk kunci berulang turut dimanfaatkan untuk meminimalkan kerentanan yang terdapat pada Vigenere [23] [24]. Penggunaan algoritma One Time Pad yang dipadukan dengan angka acak serta proses XOR dan XNOR sebagai pembentuk kunci juga dimasukkan sebagai solusi [25].

### C. Pengembangan dengan Perluasan Karakter Set

Jumlah karakter yang dikenal dalam Vigenere standar adalah dari A sampai Z sejumlah 26 karakter. Hal ini akan menjadi sulit jika akan melakukan penyandian karakter dan angka. Terlebih lagi jika informasi tersandikan mendapatkan serangan secara statistik, maka dengan 26 karakter akan lebih mudah dianalisa oleh kriptanalis. Pengembangan jumlah karakter set pada Vigenere berkembang menjadi 36 karakter yang mencakup huruf dan angka diusulkan untuk menyelesaikan permasalahan tersebut [4]. Pengembangan lain adalah penggunaan jumlah karakter set menjadi 69 jenis [26]. Dengan 69 jenis karakter yang digunakan pada Vigenere, maka Vigenere akan lebih dapat diaplikasikan pada berbagai jenis transaksi pengamanan informasi yang lebih luas. Penggunaan 95 karakter set Vigenere dilakukan untuk memperluas adaptability Vigenere pada berbagai bentuk perangkat komunikasi saat ini [2], selain itu penggunaan karakter set yang baru ini juga mendukung dalam pengamanan pertukaran informasi perbankan dan sistem saat ini [27] [28]. Hasil dari pengembangan jumlah karakter set pada Vigenere akan membentuk karakteristik cipherteks yang rumit dan akan sulit bagi pihak yang tidak berwenang untuk melakukan intervensi pertukaran informasi.

## IV. KESIMPULAN

Pengembangan Vigenere hingga saat ini masih berlanjut, sehingga akan lebih banyak keuntungan yang didapatkan dengan modifikasi pada Vigenere untuk menutup celah celah yang akan menjadikan rentan pada informasi tersandikan. Bentuk pengembangan pada Vigenere diklasifikasikan menjadi tiga bagian yakni pengembangan dengan metode Hibrid, pengembangan pada proses penerbitan kunci dan pengembangan pada penggunaan karakter setnya. Pengembangan tersebut dilakukan dengan tujuan menaikkan keamanan informasi yang disandikan dengan Vigenere Cipher. Dengan adanya penelusuran literatur tentang evolusi Vigenere Cipher, nantinya bentuk pengembangan yang lebih baik akan lebih terfokus untuk menutup celah lain yang belum dilakukan oleh para peneliti sebelumnya. Sehingga informasi rahasia akan semakin aman terhadap serangan selama proses transmisi.

## DAFTAR PUSTAKA

- [1] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *Periodicals Agency of Shanghai University, Science Press, and Springer-Verlag GmbH Germany, part of Springer Nature*, pp. 1-14, 19 August 2020.

- [2] K. Nahar and P. Chakraborty, "A Modified Version of Vigenere Cipher using 95 x 95 Table," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 5, pp. 1144-1148, 2020.
- [3] D. Rachmawati, A. Sharif and R. Sianipar, "A combination of vigenere algorithm and one time pad algorithm in the three-pass protocol," in *The 3rd Annual Applied Science and Engineering Conference (AASEC 2018)*, Bandung, Indonesia, 2018.
- [4] D. Gautam, C. Agrawal, P. Sharma, D. M. Mehta and P. Saini, "An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher," in *2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2018.
- [5] A. Subandi, M. S. Lydia, R. W. Sembiring, M. Zarlis and S. Efendi, "Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process," in *2nd Nommensen International Conference on Technology and Engineering*, Medan, Indonesia, 2019.
- [6] P. Brereton, B. . A. Kitchenham, D. Budgen, M. Turner and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571-583, 2007.
- [7] A. A. Soofi, M. I. Khan and F. E. Amin, "A Review on Data Security in Cloud Computing," *International Journal of Computer Applications*, vol. 94, no. 5, pp. 12-20, 2014.
- [8] R. S. A. Daulay, M. Zarlis and R. W. Sembiring, "Meningkatkan Keamanan Vigenere Cipher dengan Stream Cipher," in *Seminar Nasional Matematika dan Terapan*, Pematang Siantar, Indonesia, 2019.
- [9] C. A. Haris and . D. Ariyus, "Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan," *Jurnal Ilmiah Ilmu Komputer*, vol. 15, no. 2, pp. 90-96, 2020.
- [10] H. TOUIL, N. E. AKKAD and K. SATORI, "Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers," in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, Fez, Morocco, 2020.
- [11] L. Andriani, R. Rihartanto and A. B. W. Putra, "Optimasi Vigenere Cipher Menggunakan Bitswap dan Transposisi Acak pada Citra RGB," *Techno.COM*, vol. 19, no. 2, pp. 168-177, 2020.
- [12] D. . R. K. Gusti, K. A. Santoso and A. Kamsyakawuni, "VIGENERE CIPHER DENGAN MODIFIKASI PLAINTEXT," *Majalah Ilmiah Matematika dan Statistika*, vol. 20, no. 1, pp. 15-26, 2020.
- [13] H. Mawengkang, I. . L. Sitepu and S. Efendi, "Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm," in *2nd Nommensen International Conference on Technology and Engineering*, Medan, Indonesia, 2018.
- [14] I. G. A. P. Dewangga, T. W. Purboyo and R. A. Nugrahaeni, "A New Approach of Data Hiding in BMP Image Using LSB Steganography and Caesar Vigenere Cipher Cryptography," *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 10626-10636, 2017.
- [15] A. Ajmera, S. S. Ghosh and .. T. Vijayetha, "Secure LSB Steganography over Modified Vigenère-AES Cipher and Modified Interrupt Key-AES Cipher," in *IEEE Punecon*, Pune, India, 2018.
- [16] I. U. W. Mulyono, A. Susanto, T. Anggraeny and C. A. Sari, "Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit)," *KINETIK*, vol. 4, no. 1, pp. 63-74, 2019.
- [17] I. U. W. Mulyono, A. Susanto and Y. Kusumawati, "LSB STEGANO PADA KOMBINASI KRITPOGRAFI SIMETRIS CAESAR-VIGENERE," *DINAMIKA REKAYASA*, vol. 16, no. 2, pp. 139 - 146, 2020.
- [18] M. Musrini, . B. Rahardjo and R. Krisnadi, "IMPLEMENTATION OF VIGENERE CIPHER WITH EULER KEY GENERATOR TO SECURE TEXT DOCUMENT," in *1st Faculty of Industrial Technology International Congress International Conference*, Bandung, Indonesia, 2017.
- [19] D. A. Neri, R. P. Medina and A. M. Sison, "An XBOX-based key generation technique for vigenere algorithm," in *3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia, 2019.
- [20] F. Telaumbanua and T. Zebua, "Modifikasi Vigenere Cipher Dengan Pembangkit Kunci Blum Blum Shub," *KOMIK*, vol. 4, no. 1, pp. 87-91, 2020.
- [21] H. . A. Pacha, N. H. Said and A. A. Pacha, "Dynamic Generalization of the Vigenère Table based on the Logistics Map," *Malaysian Journal of Computing and Applied Mathematics*, vol. 2, no. 1, pp. 25-33, 2019.
- [22] A. Budiman and P. Paradise, "MODIFICATION OF VIGENERE ALGORITHM AND ONE TIME PAD USING RIVEST CODE 6 (RC6) KEY EXPANSION," *Compiler*, vol. 8, no. 2, pp. 149-156, 2019.
- [23] M. Ziaurrahman, E. Utami and F. W. Wibowo, "MODIFIKASI KRIPTOGRAFI KLASIK VIGENERE CIPHER MENGGUNAKAN ONE TIME PAD DENGAN ENKRIPSI BERLANJUT," *Jurnal Informasi Interaktif*, vol. 4, no. 2, pp. 63-68, 2019.
- [24] A. Rizal, . D. S. B. Utomo, R. Rihartanto, M. . E. Hiswati and H. Haviluddin, "Modified Key Using Multi-Cycle Key In Vigenere Cipher," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2S11, pp. 2600-2606, 2019.
- [25] S. . J. Siregar, M. Zarlis and Z. Situmorang, "Application and Manual Encryption Process with The Combination Algorithm of One Time Pad and Vigenere Cipher," in *International Conference on Advanced Information Scientific Development (ICAISD) 2020*, Bekasi, Indonesia, 2020.
- [26] M. S. Hossain and M. T. Islam, "An Extension of Vigenere Technique to Enhance the Security of Communication," in *2nd Int. Conf. on Innovations in Science, Engineering and Technology*, Chittagong, Bangladesh, 2018.
- [27] M. I. Z. A., S. Sutardi and Y. P. Pasrun, "IMPLEMENTASI METODE ENKRIPSI ADVANCE VIGENERE CIPHER DALAM PENGAMANAN SISTEM TRANSAKSI PAYMENT POINT ONLINE BANK," *semanTIK*, vol. 3, no. 2, pp. 237-244, 2017.
- [28] J. P. Sermenon, . K. A. S. Secugal and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *International Journal of Applied Science and Engineering*, vol. 18, no. 4, pp. 1-10, 2021.
- [29] W. M. Abdulllah and S. R. M. Zeebaree, "New Data hiding method based on DNA and Vigenere Autokey," *Academic Journal of Nawroz University*, vol. 6, no. 3, pp. 83-88, 2017.
- [30] E. Kuznetsov, "New Vigenere cipher modification," in *Conference on Mathematical Foundations of Informatics*, Chisinau, Republic of Moldova, 2018.
- [31] A. M. H. Pardede, L. P. B. Sitepu, M. Zarlis, T. Tulus, A. Iskandar, . S. Sriadhi, R. T. Manurung, N. . A. Siregar, A. E. Sari, S. Yunawati, M. Mursyidah, M. Mursalin, N. Kurniasih, C. Kurniawan and E. Winarno, "Application of Message Security Application Using Vigenere Cipher Algorithm Utilizing One Time Pad (OTP) Algorithm as a Key Generator," in *The 1st Workshop on Environmental Science, Society, and Technology*, Medan, Indonesia, 2019.