JIMP : Jurnal Informatika Merdeka Pasuruan
Vol.8 No.1 Maret 2023, P-ISSN : 2502-5716, E-ISSN : 2503-1945

Terakreditasi Peringkat Sinta 4 berdasarkan Petikan dari Keputusan Menteri Riset dan Teknologi/ Kepala Badan Riset dan Inovasi Nasional Nomor 200/M/KPT/2020, masa berlaku mulai Vol.3 No.1 tahun 2018 s.d Vol.7 No.2 tahun 2022

Meningkatkan Keamanan Pesan Rahasia pada Vigenere Cipher Menggunakan Kombinasi Caesar Cipher dan Multiple-Key

Khansa Intani[1], Gita Wulandari[2], Halimatul Hasanah[3], Ihsan L. Syarifudin[4], Eugenius M. C. Brillian[5]

[1,2,3,4,5] Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, Indonesia

[1]khansaintani@students.amikon.ac.id

[2]gitawulandari@students.amikom.ac.id

[3]halimatulhasanah@students.amikom.ac.id

[4]syarivuddin9@students.amikom.ac.id

[5]eugeniusmario05@students.amikom.ac.id

Received: 24-01-2023; Accepted: 27-08-2023; Published: 06-09-2023

Abstrak*— Kriptografi merupakan salah satu cara untuk mengamankan data yang ada. Salah satu kriptografi polyalphabetic yang populer adalah Vigenere Cipher. Akan tetapi Vigenere lemah terhadap analisa frekuensi karakter yang muncul pada ciphertext seperti Friedman dan Kasiski dikarenakan perulangan panjang key yang diperlukan untuk menyamakan panjang dengan plaintext yang digunakan. Dalam penelitian kali ini, penulis mencoba untuk meningkatkan keamanan pesan dalam penggunaan Vigenere Cipher yang dikombinasikan dengan Caesar Cipher dan penggunaan multi-key dengan panjang karakter yang berbeda-beda. Hasil dari enkripsi tersebut akan kami bandingkan dengan penggunaan Vigenere Cipher biasa menggunakan value dari Index of Coincidence dan hasil penelitian menunjukkan bahwa perulangan karakter pada ciphertext berkurang

***Kata kunci*— Vigenere Cipher, Caesar Cipher, Enkripsi, Multiple-key, Index of Coincidence**

Abstract*— Cryptography is one way to secure existing data. One of the popular polyalphabetic cryptography is the Vigenere Cipher. However, Vigenere is weak on the frequency analysis of characters that appear in ciphertexts such as Friedman and Kasiski because of the iteration of the key length required to equate length with the plaintext used. In this study, the authors tried to improve message safety in the use of Vigenere Ciphers combined with Caesar Ciphers and the use of multi-keys with different character lengths. The results of this encryption will be compared with the use of ordinary Vigenere Ciphers using the value of the Index of Coincidence and the results show that the repeatability of characters in ciphertext is reduced.

***Keyword*— Vigenere Cipher, Caesar Cipher, Encryption, Multiple-key, Index of Coincidence**

I. PENDAHULUAN

Dalam era di mana informasi yang ada dinilai sangat berharga, pihak-pihak yang tidak bertanggung jawab dapat memanfaatkan informasi tersebut dengan tujuan yang buruk[1]. Apalagi dengan maraknya penggunaan perangkat cerdas dalam kehidupan seperti Internet of Things [2]. Salah satu cara dalam mengamankan data atau informasi adalah dengan menggunakan kriptografi [3][4]. Kriptografi telah digunakan dibanyak sektor seperti pengamanan komunikasi, digital forensik, identifikasi dan autentikasi, dan meneyembunyikan data [5].Dalam penggunaannya, kriptografi memerlukan *key* dan algoritma untuk mengubah tampilan pesan menjadi tidak terbaca [6]. Selain itu, sebuah algoritma juga harus efisien, bisa diandalkan, dan mudah untuk dimengerti oleh pengirim dan penerima saat komunikasi sedang berlangsung [7]. Kriptografi terdapat dua macam yaitu monoalphabetic dan polyalphabetic. Monoalphabetic adalah metode enkripsi yang memetakan tiap-tiap abjad dengan abjad lain, berbeda dengan caesar cipher yang menggunakan metode pergeseran. Monoalphabetic menggantikan satu karakter pada plainteks menjadi satu karakter pada cipherteks. Sedangkan Polyalphabet sendiri menggunakan sejumlah monoalphabetic cipher, polyalphabetic juga dikenal sebagai sandi yang bergantung pada penggantian dan menggunakan banyak set huruf pengganti [8].

Vigenere Cipher dan Caesar Cipher termasuk di dalam polyalphabetic cipher. Vigenere Cipher merupakan polyalphabetic cipher yang paling dikenal sayangnya karena Vigenere tidak memiliki fitur difusion dan confusion, Vigenere rentan terhadap analisa frekuensi karakter yang muncul [9]. Para analis melihat dari hasil *ciphertext* apakah ada karakter yang diulang dikarenakan panjang *key* harus menyamai panjang *plaintext* di mana *key* akan diulang terus menerus untuk mengikuti panjang pesan dan dari situ mereka dapat menentukan panjang *key* yang digunakan.

Sudah ada banyak pihak yang melakukan pengembangan Vigenere Cipher salah satunya adalah dengan DNA dan Tabel Periodik yang ada dalam kimia, penggunaan karakter bahasa Myanmar, tenik LSB, dan juga chaos function [10][9][11][12][4]. Dalam jurnal ini, penulis mengembangkan Vigenere menggunakan Caesar

DOI http://dx.doi.org/10.51213/jimp.v8i1.847

Cipher dan *multiple-key*. Vigenere Cipher juga terbatas terhadap karakter yang dapat dienkripsi sehingga penambahan karakter yang ada dalam penelitian dapat digunakan sebagai salah satu untuk meningkatkan keamanan [13][6].

A. Kriptografi

Kriptografi jika dilihat dari sisi *key* terdapat dua macam, simetris dan asimetris. Dalam setiap teknik enkripsi kunci simetris, proses enkripsi dan dekripsi dilakukan menggunakan satu kunci. Algoritme ini efisien, aman, dijalankan dengan kecepatan tinggi, dan menghabiskan lebih sedikit sumber daya memori dan waktu prosesor komputer. Namun, teknik kriptografi kunci simetris mengalami kerugian dari masalah distribusi kunci, masalah manajemen kunci dan ketidakmampuan untuk menandatangani pesan secara digital. Terlepas dari kelemahan ini, banyak algoritma enkripsi kunci simetris yang aman seperti DES, TDES, Blowfish, CAST, IDEA, RC4, dan RC6 telah dikembangkan. Belakangan ini, National Institute of Standards (NIST) memilih algoritma Rijndael sebagai Advanced Encryption.

Masalah yang terkait dengan teknik kriptografi kunci simetris dipecahkan ketika mekanisme enkripsi asimetris diimplementasikan. Di sini, alih-alih satu kunci, setiap orang memiliki sepasang kunci. Satu kunci, yang disebut kunci publik, diketahui semua orang dan yang lainnya, kunci privat hanya diketahui pemiliknya. Ada hubungan matematis antara kedua kunci ini. Jadi, jika ada pesan 'm' yang dienkripsi menggunakan salah satu kunci, pesan tersebut dapat didekripsi oleh bagian lainnya. Berbagai algoritma enkripsi asimetris (RSA, Elgamal) telah diimplementasikan. Detail tentang cara kerja teknik enkripsi asimetris dapat diperoleh dari Schneier, Stallings. Algoritma enkripsi asimetris secara luas dibagi menjadi tiga keluarga: 1. Algoritma berdasarkan Masalah faktorisasi bilangan bulat (misalnya RSA) 2. Algoritma berdasarkan masalah logaritma diskrit [14].

B. Vigenere Cipher

Teknik Vigenere Cipher mengenkripsi teks abjad dengan bantuan berbagai sandi Caesar berdasarkan huruf dari beberapa *key*. Vigenere cipher terdiri dari banyak Caesar cipher dengan nilai pergeseran yang berbeda.Vigenere Cipher juga dikenal sebagai cipher substitusi alfabet yang merupakan matriks pergeseran sandi 26 x 26 Caesar[15].

Algoritma Vigenere memiliki tingkat keamanan yang lemah karena menggunakan alfabet numerik yang berjumlah 26 karakter sedangkan untuk koma, tanda baca, titik, dan simbol lainnya digunakan sebagai *key* saja. Sehingga memudahkan penyerang dalam menyerang dan menyebarkan informasi karena tekniknya yang sangat mudah dipecahkan [8]. Formula matematika untuk enkripsi dan dekripsi Vigenere dapat dilihat pada formula (1) dan (2).

$$C_i = (P_i + k_i)\ mod\ 26 \quad (1)$$

$$P_i = (C_i - k_i)\ mod\ 26 \quad (2)$$

Di mana C_i merupakan *ciphertext* posisi ke-i, P_i adalah posisi *plaintext* ke-i, k_i adalah posisi *key* ke-i.

C. Caesar Cipher

Dalam teknik Caesar cipher setiap huruf digeser ke beberapa tempat, pola dalam teks sandi sama dengan panjang kata kunci yang digunakan. Formula matematika untuk enkripsi dan dekripsi dapat dilihat pada formula (3) dan formula (4).

$$C_i = (P_i + k)\ mod\ 26 \quad (3)$$

$$P_i = (C_i - k)\ mod\ 26 \quad (4)$$

Di mana C_i merupakan *ciphertext* posisi ke-i, P_i adalah posisi *plaintext* ke-i, *k* merupakan besar dari nilai pergeseran.

D. Index of Coincidence

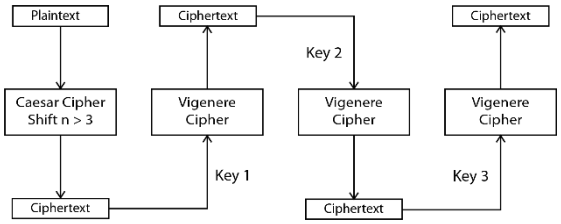
Untuk memproses Vigenere Cipher diperlukan tiga langkah yaitu mendapatkan *key*, mennetukan panjang *key* dan terakhir menentukan jumlah karakter *key* [16]. Rumus untuk medapatkan value dari Index of Coincidence dapat dilihat pada formula 5 berikut.

$$IC = \sum_{i=A}^{i=Z} \frac{n_i(n_i-1)}{N(\ \ )N-1} \quad (5)$$

Di mana n_i merupakan jumlah kemunculan dari huruf i dalam teks dan N merupakan total huruf yang ada di *ciphertext*.

II. METODOLOGI PENELITIAN

Proses enkripsi yang akan dilakukan pada penelitian ini dapat dilihat pada Gambar. 1.



Gambar. 1 Skema enkripsi menggunakan Vigenere, Caesar dan *multiple-key*

Langkah pertama yang dilakukan adalah melakukan enkripsi menggunakan Caesar Cipher menggunakan nilai pergeseran lebih dari 3. Hasil dari enkripsi tersebut akan digunakan sebagai *plaintext* untuk enkripsi Vigenere Cipher. Jumlah karakter yang digunakan adalah 94 karakter, termasuk tanda baca dan spasi.

Selanjutnya adalah melakukan enkripsi menggunakan Vigenere Cipher. Dalam penelitian kali ini dilakukan 3 kali enkripsi dengan menggunakan tiga buah *key* dengan panjang karakter yang berbeda-beda. Sama seperti Caesar Cipher sebelumnya, hasil enkripsi akan menjadi *plaintext* untuk enkripsi selanjutnya. Sehingga dalam penelitian kali ini satu *plaintext* akan mengalami enkripsi sebanyak empat kali.

Ciphertext akan dibandingkan dengan menggunakan Index of Coincidence. Semakin kecil IC menunjukkan

DOI http://dx.doi.org/10.51213/jimp.v8i1.847

bahwa perulangan karakter dalam *ciphertext* lebih sedikit sehingga dapat mencegah analisa panjang *key* dengan melihat perulangan karakter yang ada. Dalam penelitian ini, terdapat dua metode sebagai perbandingan, enkripsi hanya menggunakan *multiple-key* dan Vigenere serta enkripsi menggunakan Caesar, *multiple-key* dan Vigenere. Untuk proses dekripsi merupakan kebalikan dari proses enkripsi.

III. HASIL DAN PEMBAHASAN

Diberikan sebuah *plaintext* berupa 'Universitas Warna Ungu di Jogja!'. *Plaintext* tersebut akan dienkripsikan menggunakan Caesar Cipher dengan nilai pergeseran sebesar 5. Di dapatkan *ciphertext* berupa 'ZsnAjwxnyfx5"fwsf5Zslz5in5Otlof&'. *Ciphertext* tersebut akan dienkripsi kembali menggunakan Vigenere Cipher menggunakan tiga buah *key* dengan panjang karakter sebesar 5, 8, dan 15. Pada Tabel I terdapat *key* dan hasil enkripsi dari metode yang diusulkan, yaitu Caesar Cipher, *multiple-key* dan Vigenere Cipher.

TABEL I
HASIL ENKRIPSI DARI METODE YANG DIUSULKAN

Vigenere Cipher + Caesar Cipher + *Multiple-key*		
Key		***Ciphertext***
5 karakter	Bung4	4WKQn("KOj)z]vA$Js:wW$syrG=QBsQ3
8 karakter	Mat4hari	Q'.UE<{#4t5D9F"@~CcA..TQ.QfUSC<l
15 karakter	Bung4 Mataha12i	`44+I<I-xDmNaH>qtZsE.t$>\(pVUUmP

Selanjutnya adalah melakukan enkripsi menggunakan metode ke-dua sebagai pembanding dari metode yang diusulkan, yaitu enkripsi Vigenere menggunakan *multiple-key* dengan *plaintext* dan *key* yang sama seperti sebelumnya. Hasil enkripsi dari metode tersebut dapat dilihat pada Tabel II.

TABEL III
HASIL ENKRIPSI DARI VIGENERE CIPHER MENGGUNAKAN *MULTIPLE-KEY*

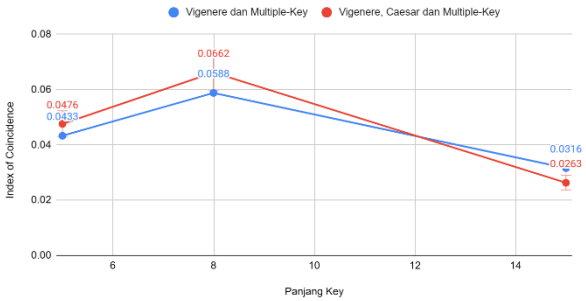
Vigenere Cipher + Caesar Cipher + *Multiple-key*		
Key		***Ciphertext***
5 karakter	Bung4	~RFLi#WFJe$u>qvYEn+rRYntmB.LwnL}
8 karakter	Mat4hari	L")Pz-\X~o0y4AW;_x7v))OL)LaPNx-g
15 karakter	Bung4 Mataha12i	[~~&D-D(syhI5C/loUnz)oY/=#kQPPhK

Hasil dari enkripsi di kedua tabel tersebut akan dibandingkan dengan menggunakan IC. Hasil dari IC dapat dilihat pada Tabel III.

TABEL IIIII
HASIL ENKRIPSI DARI VIGENERE CIPHER MENGGUNAKAN *MULTIPLE-KEY*

Metode	**Panjang *Key***	**IC**
Vigenere menggunakan *multiple-key*	5	0.0433
	8	0.0588
	15	0.0316
Vigenere menggunakan Caesar dan *multiple-key*	5	0.0476
	8	0.0662
	15	0.0263

Dapat dilihat pada Tabel 3 bahwa pada proses enkripsi Vigenere dengan menggunakan *key* pertama, IC milik Vigenere dan *multiple-key* memiliki nilai yang lebih rendah dibandingkan IC milik Vigenere dengan Caesar dan *multiple-key*. Sedangkan IC milik Vigenere dengan Caesar dan *multiple-key* dengan jumlah karakter 15 lebih rendah dari pada milik Vigenere dengan *multiple-key* yaitu 0.0263 seperti yang dilihat pada Tabel 3 dan Gambar. 2 berikut.



Gambar. 2 Grafik perbanding nilai Index of Coincidence

Dari grafik tersebut dapat dilihat bahwa value IC dari Vigenere dan *Multiple-key* lebih tinggi dibandingkan dengan IC dari metode yang diusulkan. Akan tetapi pada hasil enkripsi terakhir, didapat IC milik metode yang diusulkan lebih rendah dari pada IC milik Vigenere dan *multiple-key*.

IV. KESIMPULAN

Metode yang diusulkan memiliki nilai IC yang lebih rendah pada hasil enkripsi akhir yaitu sebesar 0.0263. IC yang rendah menunjukkan bahwa peluang dari karakter yang diulang di dalam suatu *ciphertext* lebih kecil sehingga dapat menghindari dari analisa *ciphertext* untuk menemukan panjang *key* yang digunakan.

REFERENSI

[1] A. L. Latifah, Lembaga Ilmu Pengetahuan Indonesia. Research Center for Informatics, Institute of Electrical and Electronics Engineers. Indonesia Section, dan Institute of Electrical and Electronics Engineers, 2018 International Conference on Computer, Control, Informatics and its Applications : "Recent Challenges in Machine Learning for Computing Applications" : proceedings : November 1st-2nd, 2018, Tangerang, Indonesia.

[2] 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, 2019.

[3] IEEE Staff, 2019 3rd International Conference on Informatics and Computational Sciences (ICICoS). IEEE, 2019.

[4] R. Hammad dkk., "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message," dalam Journal of Physics: Conference Series, 2022, vol. 2279, no. 1. doi: 10.1088/1742-6596/2279/1/012006.

DOI http://dx.doi.org/10.51213/jimp.v8i1.847

[5] A. Al-Sabaawi, "Cryptanalysis of Vigenère Cipher: Method Implementation," dalam 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2020, Des 2020. doi: 10.1109/CSDE50874.2020.9411383.
[6] K. Nahar dan P. Chakraborty, "A Modified Version of Vigenere Cipher using 95 95 Table," Int J Eng Adv Technol, vol. 9, no. 5, hlm. 1144–1148, Jun 2020, doi: 10.35940/ijeat.E9941.069520.
[7] International Islamic University Chittagong, Institute of Electrical and Electronics Engineers. Bangladesh Section, dan Institute of Electrical and Electronics Engineers, 2018 International Conference on Innovations in Science, Engineering and Technology : ICISET 2018 : International Islamic University Chittagong, Chittagong, Bangladesh : 27-28 October 2018.
[8] D. Gautam, P. Sharma, C. Agrawal, M. Mehta, dan P. Saini, "An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher," 2018.
[9] Sri Shakthi Institute of Engineering and Technology, Institute of Electrical and Electronics Engineers. Madras Section, India Electronics & Semiconductor Association, dan Institute of Electrical and Electronics Engineers, 2019 International Conference on Computer Communication and Informatics : January 23-25, 2019, Coimbatore, India.
[10] L. Voleti, R. M. Balajee, S. K. Vallepu, K. Bayoju, dan D. Srinivas, "A Secure Image Steganography Using Improved Lsb Technique and Vigenere Cipher Algorithm," dalam Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021, Mar 2021, hlm. 1005–1010. doi: 10.1109/ICAIS50930.2021.9395794.
[11] Arab Computer Society, IEEE Computer Society, dan Institute of Electrical and Electronics Engineers., 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications : October 28th to November 1st, 2018, Aqaba, Jordan.
[12] B. Triandi, E. Ekadiansyah, R. Puspasari, L. T. Iwan, dan F. Rahmad, "Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions."
[13] A. Rizal, D. S. B. Utomo, R. Rihartanto, M. E. Hiswati, dan H. Haviluddin, "Modified *key* using multi-cycle *key* in vigenere cipher," International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special Issue 11, hlm. 2600–2606, Sep 2019, doi: 10.35940/ijrte.B1313.0982S1119.
[14] C. R. S. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols." [Daring]. Available: www.iosrjournals.orgwww.iosrjournals.org
[15] A. Ajmera, S. S. Ghosh, dan V. T. Asst, "Secure LSB Steganography over Modified Vigenère-AES Cipher and Modified Interrupt *Key*-AES Cipher."
[16] A. Al-Sabaawi, "Cryptanalysis of Vigenère Cipher: Method Implementation," dalam 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2020, Des 2020. doi: 10.1109/CSDE50874.2020.9411383.

DOI http://dx.doi.org/10.51213/jimp.v8i1.847