

BAB V PENUTUP

5.1 Kesimpulan

Dari hasil penelitian dan perbandingan IoC dari Basic Vigenere, Developed Vigenere, dan Developed Vigenere with Shuffled Key yang dilakukan dapat disimpulkan bahwa panjang kunci memengaruhi Index of Coincidence. Hal ini ditunjukkan dengan garis yang menunjukkan nilai IoC hasil enkripsi dengan panjang kunci yang ditunjukkan pada sumbu X. Semakin panjang kunci yang digunakan untuk enkripsi, semakin berkurang juga banyak karakter yang muncul berulang kali. Hal tersebut tidak hanya berlaku pada penggunaan Vigenere asli, yaitu 26 karakter, tetapi juga pada penggunaan Vigenere yang dikembangkan menggunakan 95 karakter dan juga yang dikombinasikan dengan karakter kunci yang diacak.

Perluasan karakter yang digunakan pada Vigenere cipher, yang awalnya berupa 26 karakter menjadi 95 karakter juga memengaruhi nilai Index of Coincidence. Pada hasil penelitian dan perbandingan juga dapat dilihat bahwa IoC yang dimiliki oleh Vigenere asli lebih besar dibandingkan IoC yang dimiliki oleh Vigenere yang dikembangkan. Index of Coincidence yang dimiliki oleh Vigenere asli dengan kunci yang digunakan berada pada *range* 0.0514 sampai 0.0364. Jika mengacu pada Parameter Pengujian, jika n atau nilai dari IoC berada di antara 0.0385 sampai 0.065, $0.0385 \leq n \leq 0.065$, *ciphertext* tersebut memiliki kemungkinan didekripsi menggunakan *polyalphabetic cipher* yang mana Vigenere merupakan salah satu dari *polyalphabetic cipher*. Penggunaan kunci dengan panjang 13 pada Vigenere asli dapat membuat IoC berada di luar *range* tersebut, menunjukkan bahwa terdapat kemungkinan apabila kunci yang digunakan lebih panjang dari 13 dapat membuat kriptanalisis menghadapi tantangan yang lebih besar dalam upaya mereka untuk mendekripsi *ciphertext*. Hal yang sama juga terjadi pada Vigenere dengan perluasan karakter. Di mana IoC yang diperoleh berada di luar *range* tersebut.

Penggunaan kunci yang dilakukan substitusi dengan karakter yang diacak

juga berpengaruh pada keamanan teks. Apabila kunci asli tersebar dan dilakukan dekripsi pada *ciphertext*, *plaintext* yang didapatkan tidak sesuai dengan pesan sesungguhnya. Sehingga penggunaan kunci yang dienkripsi juga dapat meningkatkan keamanan dari pesan.

5.2 Saran

Apabila dilakukan penelitian selanjutnya, list karakter yang digunakan untuk melakukan substitusi dari kunci dapat menjadi salah satu fokus utama. Seperti bagaimana cara mengirim 95 karakter dengan posisi acak kepada penerima dengan efektif, misal menambahkan susunan karakter yang digunakan sebagai substitusi untuk kunci pada *ciphertext*. Hal ini dikarenakan pada proses enkripsi menggunakan algoritma Vigenere yang dikembangkan, kunci yang digunakan adalah kunci yang telah terenkripsi. Jadi apabila 95 karakter yang diacak tersebut tersebar dapat membuat kriptanalisis melakukan dekripsi dengan mudah. Peneliti juga dapat menggunakan perluasan karakter dengan karakter-karakter yang lebih banyak. Seperti menggunakan emoji atau aksara-aksara daerah tertentu.

