MODIFIKASI ALGORITMA KRIPTOGRAFI KLASIK VIGENERE *CIPHER* DIPERKUAT DENGAN AFFINE *CIPHER* DAN CAESAR *CIPHER*

Nama Mahasiswa	: Fikri Catur Wijayanto
NIM	: 02171009
Dosen Pembimbing Utama	: Aditya Putra Pratama, S.Si., M.Si.
Dosen Pembiming Pendamping	: Sigit Pancahayani, S.Si., M.Si.

ABSTRAK

Pertukaran data dan informasi merupakan hal yang sering dilakukan, banyak informasi penting rentan untuk diketahui sehingga dibutuhkan metode untuk melindungi informasi tersebut. Adapun ilmu yang digunakan untuk mengamankan dan menjaga kerahasian informasi tersebut, yaitu kriptografi. Berdasarkan perkembangan dan sejarahnya kriptografi memiliki tiga kategori yaitu kriptografi klasik, kriptografi modern dan kriptografi kuantum. Seiring dengan perkembangan teknologi, kriptografi klasik mulai jarang digunakan dikarenakan tingkat keamanannya yang rendah. Beberapa penelitian dilakukan dalam memodifikasi algoritma kriptografi klasik dengan tujuan untuk meningkatkan keamanan dari kriptografi klasik, salah satu penelitian yang dilakukan oleh Juliadi, Prihandono, & Kusumastuti (2013) membahas mengenai modifikasi Affine *cipher* yang diperkuat dengan Vigenere *cipher*. Pada penelitian ini dilakukan modifikasi kriptografi klasik menggunakan algoritma Vigenere *cipher* yang diperkuat oleh Affine *cipher* dan Caesar *cipher* yang diharapkan dapat meningkatkan kemanan dari kriptografi klasik sebagai mitigasi serangan *cyber*. Dari pengembangkan kriptografi klasik pada penelitian ini didapat dua algoritma modifikasi yaitu VAC dan VCA *cipher*. VAC dan VCA *cipher* memiliki tingkat keamanan yang sama dimana jika seorang kripanalis ingin memcahkan kunci *cipher* diperlukan percobaan sebanyak $(128 \times 8192 \times \sum_{j=1}^{k} 128^{j} \times 128!)$ percobaan. Berdasarkan hasil simulasi sebanyak 5 kali, diperoleh rata-rata *error* VAC *cipher* sebesar 1.232% dan VCA *cipher* sebesar 1.62% yang berarti hanya sedikit karakter yang terjadi mengalami kesalahan dekripsi text. Didapatkan hasil rata-rata waktu *running* saat proses enkripsi VAC dan VCA cipher adalah 0,001165 detik dan 0,000927 detik, kemudian didapatkan hasil rata-rata waktu *running* saat proses dekripsi VAC dan VCA cipher adalah 0,003234 detik dan 0,003089 detik

Kata Kunci: Affine *cipher*, algoritma, Caesar *cipher*, kriptografi, dan Vigenere *cipher*