

**APLIKASI KOMBINASI METODE *VIGENERE CIPHER* DAN METODE
AFFINE CIPHER PADA KRIPTOGRAFI**

SKRIPSI

**Sebagai Salah Satu Syarat untuk Memperoleh Gelar
Sarjana Sains Bidang Studi Matematika**



**Oleh :
AZHIMI
NIM. 08121001009**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS SRIWIJAYA
AGUSTUS 2017**

LEMBAR PENGESAHAN

**APLIKASI KOMBINASI METODE *VIGENERE CIPHER* DAN METODE
AFFINE CIPHER PADA KRIPTOGRAFI**

SKRIPSI

**Sebagai Salah Satu Syarat Memperoleh Gelar
Sarjana Sains Bidang Studi Matematika**

Oleh :

**AZHIMI
NIM. 08121001009**

Pembimbing Pembantu

**Inderalaya, Agustus 2017
Pembimbing Utama**

**Evi Yuliza, M.Si
NIP. 19780727 200801 2 012**

**Indrawati, M.Si
NIP. 19710610 199802 2 001**

**Mengetahui,
Ketua Jurusan Matematika**

**Drs. Sugandi Yahdin, M.M
NIP. 19580727 198603 1 003**

LEMBAR PERSEMBAHAN

Motto :

*“Siapapun yang menempuh suatu jalan untuk mendapatkan ilmu, maka Allah akan memberikan kemudahan jalannya menuju surga”
(H.R. Muslim)*

*“Open your heart, open you mind. Do the best”
(Edi Vatoni)*

“Jangan berhenti untuk melakukan kebaikan”

Skripsi ini Kupersembahkan kepada :

- ❖ Bapak dan Ibu tercinta*
- ❖ Kakakku yang tersayang*
- ❖ Dosen dan Guruku*
- ❖ Sahabat-Sahabat Terbaik ku, dan*
- ❖ Almamater ku*

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji syukur kehadiran Allah SWT Yang Maha Pengasih lagi Maha Penyayang atas segala limpahan rahmat, karunia, serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang telah direncanakan dengan judul “**Aplikasi Kombinasi Metode Vigenere Cipher dan Metode Affine Cipher pada Kriptografi**”. Shalawat serta salam semoga senantiasa tercurahkan kepada Nabi Besar kita Nabi Muhammad SAW beserta seluruh keluarga dan sahabatnya yang telah membawa kita dari zaman kebodohan ke zaman yang terang benderang.

Dengan penuh rasa hormat, cinta, kasih sayang dan kerendahan hati, penulis mempersembahkan skripsi ini khusus untuk kedua orang tua tercinta, terkasih dan tersayang **Bapak Warlidilah** dan **Ibu Suknah** yang telah merawat dan mendidik penulis dengan penuh rasa cinta dan kasih sayang, serta dukungan yang sangat berharga berupa motivasi keluarga, do'a, perhatian, semangat, serta material untuk penulis selama ini.

Penulis menyadari bahwa keberhasilan penyusunan skripsi ini tidak terlepas dari bantuan pembimbing, dan berbagai pihak lain baik langsung maupun tidak langsung. Dalam kesempatan ini, penulis ingin menyampaikan terimakasih kepada :

1. Ibu **Indrawati, M.Si** selaku Dosen Pembimbing Utama yang telah bersedia meluangkan waktu dengan penuh kesabaran dan perhatian dalam memberikan banyak ide pemikiran, bimbingan, nasehat, pengarahan, serta kritik dan saran yang sangat berguna bagi penulis selama pengerjaan skripsi sehingga skripsi

ini dapat terselesaikan dengan baik dan sesuai dengan waktu yang direncanakan.

2. Ibu **Evi Yuliza, M.Si** selaku Dosen Pembimbing Pembantu yang juga telah banyak memberikan arahan dan bimbingan kepada penulis selama pengerjaan skripsi ini maupun selama belajar di Jurusan Matematika FMIPA Universitas Sriwijaya.
3. Bapak **Alfensi Faruk, S.Si., M.Sc** selaku Dosen Pembimbing Akademik yang telah banyak memberikan arahan dan bimbingan kepada penulis selama belajar di Jurusan Matematika FMIPA Universitas Sriwijaya.
4. Bapak **Drs. Endro Setyo Cahyono, M.Si**, Ibu **Dra. Ning Eliyati, M.Pd**, dan Ibu **Irmeilyana, S.Si., M.Si** selaku Dosen Penguji Utama yang telah bersedia meluangkan waktunya dalam memberikan tanggapan, kritik serta saran yang bermanfaat dalam perbaikan penyelesaian skripsi ini.

Selain itu, penulis juga mendapatkan dukungan dari pihak-pihak lain selama masa perkuliahan hingga penyelesaian skripsi ini. Oleh karena itu, penulis juga ingin mengucapkan terima kasih kepada :

1. Bapak **Drs. Sugandi Yahdin, M.M** selaku Ketua Jurusan Matematika FMIPA Universitas Sriwijaya.
2. Seluruh **Dosen di Jurusan Matematika FMIPA Universitas Sriwijaya, Guru-Guru di SMA Negeri 1 Kuala Tungkal, SMP Negeri 2 Kuala Tungkal, dan SD Negeri 1 Kuala Tungkal**. Terima kasih atas ilmu yang telah diberikan selama proses pendidikan.

3. Kakakku **Hici Swarni**, terima kasih atas semangat, do'a, motivasi dan dukungan yang telah diberikan.
4. Sahabat terbaikku "COEG", **Amira Fitri Adila, Ahmad Junaidi, Defita Yolanda, Dewi Rakhmatia Nur, Ismail, M. Ario Wibowo, Rakhatama Gusri, dan Ramadhan Pratama**, terima kasih buat canda dan tawa kalian dan kebersamaan kita selama ini, semoga kita menjadi sahabat selamanya.
5. Sahabat-sahabat seperjuangan: **Akbar Yulanda, M. Syahrival. A, Emi Widarti, Nelda Amelia, M. Allbar Pratama, Reyfaldo Tomy, Atoihilah Abdul Latif, Dian Permata Sari, Triyani, Titi Larastiana, Adela Rosita**, dan seluruh teman-teman Angkatan 2012, terima kasih untuk semua canda tawa, suka duka, nasehat, semangat, dukungan, cita-cita dan harapan yang telah kita lewati bersama. Semoga persahabatan ini tidak berakhir sampai disini, tetapi terus terjalin selama-lamanya, karena kita adalah keluarga.
6. **Kakak tingkat Angkatan** 2009, 2010, 2011 serta **adik tingkat Angkatan** 2013, 2014, 2015 dan 2016 atas segala bentuk *support* yang telah diberikan.
7. **Sabeum Ratu Yuliana, Sabeum Anjaz Z** dan para **Taekwondo UNSRI** atas bantuan dalam segala bentuk selama ini.
8. **Sri Erlita**, yang memberikan semangat, bantuan, kasih sayang dan perhatiannya selama ini.
9. **Ahmad Fauzan**, atas dukungan, semangat, saran dan kritiknya.
10. **Kak Iwan, dan Bu Hamidah** yang telah banyak membantu dalam proses administrasi.

11. Semua pihak yang tidak dapat penulis sebutkan satu-persatu yang telah memberikan do'a, dukungan dan masukan yang berguna untuk menyelesaikan skripsi ini. Semoga segala kebaikan dan pertolongan semuanya mendapatkan berkah dari Allah SWT.

Akhir kata dengan segala kerendahan hati, mohon maaf apabila masih banyak kekurangan dalam penyusunan skripsi ini dan masih jauh dari kesempurnaan, maka saran dan kritik yang membangun dari semua pihak sangat diharapkan demi penyempurnaan selanjutnya. Semoga skripsi ini dapat menambah pengetahuan dan bermanfaat bagi semua pihak yang memerlukan. Aamiin.

Wassalamu'alaikum Wr. Wb

Indralaya, Agustus 2017

Penulis

THE APPLICATION COMBINATION OF *VIGENERE CIPHER* METHOD AND *AFFINE CIPHER* METHOD IN CRYPTOGRAPHY

By:
AZHIMI
08121001009

ABSTRACT

Cryptography has two main concepts in the process namely the process of encryption and decryption process. The method used in this research is *Vigenere Cipher* method and *Affine Cipher* method. This research combines *Vigenere Cipher* method and *Affine Cipher* method. First determine the desired *Plaintext*, then determine the *Key* used. In this combination requires 4 *Key* which consists of 2 *Key* for *Vigenere Cipher* method and 2 *Key* for *Affine Cipher* method. *Vigenere Cipher* method performs 2 times encryption process and 2 times decryption process because it has 2 *Key*, while *Affine Cipher* method perform once encryption process and once decryption process with 2 *Key* at once. In the encryption process, the *Vigenere Cipher* method is done at the beginning, then the results are re-encrypted using *Affine Cipher* method and obtained *Ciphertext*, while in the decryption, *Affine Cipher* method is done at the beginning, then the results are redefined by using *Vigenere Cipher* method and obtained *Plaintext*. Total encoding process is 6 process consisting 3 encryption process and 3 decryption process with 4 *Key* which is used, although different length of *Plaintext* and different *Key*.

Keywords: Cryptography, Vigenere, Affine, Encryption, Decryption, Combination

APLIKASI KOMBINASI METODE *VIGENERE CIPHER* DAN METODE *AFFINE CIPHER* PADA KRIPTOGRAFI

**Oleh :
AZHIMI
08121001009**

ABSTRAK

Kriptografi memiliki dua konsep utama dalam prosesnya yakni proses enkripsi dan proses dekripsi. Metode yang digunakan dalam penelitian ini adalah metode *Vigenere Cipher* dan metode *Affine Cipher*. Penelitian ini mengkombinasikan metode *Vigenere Cipher* dan metode *Affine Cipher*. Terlebih dahulu menentukan *Plaintext* yang diinginkan, selanjutnya menentukan *Key* yang digunakan. Dalam kombinasi ini memerlukan 4 *Key* yang terdiri dari 2 *Key* untuk metode *Vigenere Cipher* dan 2 *Key* metode *Affine Cipher*. Metode *Vigenere Cipher* melakukan 2 kali proses enkripsi dan 2 kali proses dekripsi karena memiliki 2 *Key*, sedangkan metode *Affine Cipher* melakukan sekali proses enkripsi dan sekali proses dekripsi dengan 2 *Key* sekaligus. Pada proses enkripsi, metode *Vigenere Cipher* dilakukan di awal, lalu hasilnya dienkripsikan kembali dengan menggunakan metode *Affine Cipher* dan didapatkan *Ciphertext*, sedangkan pada proses dekripsi, metode *Affine Cipher* dilakukan di awal, lalu hasilnya didekripsikan kembali dengan metode *Vigenere Cipher* dan didapatkan *Plaintext*. Total proses penyandian adalah 6 proses yang terdiri 3 proses enkripsi dan 3 proses dekripsi, serta 4 *Key* yang digunakan, meskipun berbeda panjang *Plaintext* dan berbeda *Key*.

Kata kunci: Kriptografi, *Vigenere*, *Affine*, *Cipher*, Kombinasi, Enkripsi, Dekripsi

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERSEMBAHAN DAN MOTTO	iii
KATA PENGANTAR	iv
ABSTRACT	viii
ABSTRAK	ix
DAFTAR ISI	x
DAFTAR TABEL	xiii
BAB I PENDAHULUAN	
1.1. Latar Belakang	1
1.2. Perumusan Masalah	2
1.3. Pembatasan Masalah	3
1.4. Tujuan	3
1.5. Manfaat	3
BAB II TINJAUAN PUSTAKA	
2.1. Kriptografi	4
2.2. <i>Modulo</i>	6
2.2.1. Teori <i>Modulo</i>	7
2.2.2. Invers <i>Modulo</i>	7
2.3. Bilangan Prima	7
2.4. Metode <i>Vigenere Cipher</i>	8

2.5. Metode <i>Affine Cipher</i>	9
BAB III METODOLOGI PENELITIAN	
3.1. Tempat	11
3.2. Waktu	11
3.3. Metode Penelitian	11
BAB IV HASIL DAN PEMBAHASAN	
4.1. Penentuan <i>Modulo</i> dan Inversnya.....	12
4.2. Metode <i>Vigenere Cipher</i>	13
4.2.1. Proses Enkripsi Metode <i>Vigenere Cipher</i>	13
4.2.2. Proses Dekripsi Metode <i>Affine Cipher</i>	17
4.3. Metode <i>Affine Cipher</i>	20
4.3.1. Proses Enkripsi Metode <i>Affine Cipher</i>	20
4.3.2. Proses Dekripsi Metode <i>Affine Cipher</i>	22
4.4. Kombinasi Metode <i>Vigenere Cipher</i> dan Metode <i>Affine Cipher</i>	24
4.5. Contoh Penerapan Kombinasi Metode <i>Vigenere Cipher</i> dan Metode <i>Affine Cipher</i>	25
4.5.1. Proses Enkripsi Kombinasi dengan Metode <i>Vigenere Cipher</i> ...	26
4.5.2. Proses Enkripsi Kombinasi dengan Metode <i>Affine Cipher</i>	32
4.5.3. Proses Dekripsi Kombinasi dengan Metode <i>Affine Cipher</i>	36
4.5.4. Proses Dekripsi Kombinasi dengan Metode <i>Vigenere Cipher</i> ...	38
BAB V KESIMPULAN DAN SARAN	
5.1. Kesimpulan	45
5.2. Saran	45

DAFTAR PUSTAKA 46

DAFTAR TABEL

	Halaman
Tabel 2.1 Penginisialan Huruf Alfabet menjadi Angka 0- 25	6
Tabel 4.1 Invers Bilangan pada <i>Modulo</i> 40	13
Tabel 4.2 Aturan Konversi	15
Tabel 4.3 Proses Enkripsi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 1	16
Tabel 4.4 Proses Enkripsi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 2	17
Tabel 4.5 Proses Dekripsi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 2	19
Tabel 4.6 Proses Dekripsi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 1	20
Tabel 4.7 Proses Enkripsi Metode <i>Affine Cipher</i> dengan <i>a</i> dan <i>b</i>	22
Tabel 4.8 Proses Dekripsi Metode <i>Affine Cipher</i> dengan <i>a</i> dan <i>b</i>	24
Tabel 4.9 Proses Enkripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 1 (Contoh 1)	27
Tabel 4.10 Proses Enkripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 1 (Contoh 2)	28
Tabel 4.11 Proses Enkripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 1 (Contoh 3)	29
Tabel 4.12 Proses Enkripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 2 (Contoh 1)	30
Tabel 4.13 Proses Enkripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 2 (Contoh 2)	31
Tabel 4.14 Proses Enkripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key</i> 2 (Contoh 3)	32

Tabel 4.15 Proses Enkripsi Kombinasi <i>Affine Cipher</i> dengan <i>Key 3</i> dan <i>Key 4</i> (Contoh 1)	33
Tabel 4.16 Proses Enkripsi Kombinasi <i>Affine Cipher</i> dengan <i>Key 3</i> dan <i>Key 4</i> (Contoh 2)	34
Tabel 4.17 Proses Enkripsi Kombinasi <i>Affine Cipher</i> dengan <i>Key 3</i> dan <i>Key 4</i> (Contoh 3)	35
Tabel 4.18 Proses Dekripsi Kombinasi dengan Metode <i>Affine Cipher</i> (Contoh 1).....	36
Tabel 4.19 Proses Dekripsi Kombinasi dengan Metode <i>Affine Cipher</i> (Contoh 2).....	37
Tabel 4.20 Proses Dekripsi Kombinasi dengan Metode <i>Affine Cipher</i> (Contoh 3).....	38
Tabel 4.21 Proses Dekripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key 2</i> (Contoh 1)	39
Tabel 4.22 Proses Dekripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key 2</i> (Contoh 2)	40
Tabel 4.23 Proses Dekripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key 2</i> (Contoh 3)	41
Tabel 4.24 Proses Dekripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key 1</i> (Contoh 1)	42
Tabel 4.25 Proses Dekripsi Kombinasi Metode <i>Vigenere Cipher</i> dengan <i>Key 1</i> (Contoh 2)	43

Tabel 4.26 Proses Dekripsi Kombinasi Metode *Vigenere Cipher* dengan *Key* 1

(Contoh 3) 44

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di zaman sekarang seiring meningkatnya teknologi, keamanan suatu pesan rahasia sangatlah penting agar sampai pada penerima pesan dengan aman. Kriptografi adalah ilmu dan seni menjaga keamanan pesan (Munir, 2006). Ilmu kriptografi ini sudah diterapkan untuk mengirim pesan rahasia pada zaman Romawi di era raja *Julius Caesar*.

Kriptografi memiliki dua konsep utama dalam prosesnya yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi awal (*Plaintext*) diubah menjadi informasi yang tidak dikenali atau tersamarkan (*Ciphertext*), sedangkan dekripsi adalah proses kebalikan dari enkripsi yaitu mengubah *Ciphertext* menjadi *Plaintext*. Metode-metode yang ada di kriptografi antara lain: *Caesar*, *Affine*, *Monoalphabetic*, *Polyalphabetic*, *Vigenere*, *Beaufort*, *Playfair*, Transposisi, MD5, DES, RSA, DSA, ElGamal dan SHA.

Metode *Affine* adalah perluasan dari metode *Caesar* yang mengalihkan *Plaintext* dengan sebuah angka dan menambahkannya dengan sebuah pergeseran. Sedangkan metode *Vigenere* adalah metode yang menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. Metode ini juga dipublikasikan oleh diplomat sekaligus kriptologis di Prancis, yaitu Blaise de

Vigenere. Metode *Vigenere* menggunakan tabel *Vigenere* untuk melakukan enkripsi dan dekripsi

Septiarini dan Hamdani (2011) telah membuat program untuk membuat pesan rahasia dengan metode *Affine*. Dengan menggunakan metode *Affine* ini dapat dibuat pesan rahasia yang susah untuk dipecahkan karena menggunakan dua kunci untuk menyelesaikannya yaitu berupa bilangan prima yang memiliki jumlah yang terbatas.

Hamdani (2012) telah membuat program pesan rahasia dengan metode *Vigenere*. Dalam penelitiannya terdapat hanya satu kunci yang digunakan untuk membuat pesan rahasia. Namun, kebebasan dalam mengisi data kunci tanpa dibatasi panjang kata kunci dan jenis karakternya, baik huruf maupun angka.

Sulasdianti (2014) telah mengkombinasikan metode *Vigenere Cipher* dan metode *Cipher Hill*. Dalam penelitian ini didapatkan suatu pesan rahasia yang susah untuk dipecahkan karena menggunakan dua metode. Kunci yang digunakan lebih dari tiga kunci.

Berdasarkan latar belakang tersebut, pada penelitian ini dibahas kombinasi metode *Vigenere Cipher* dan metode *Affine Cipher*.

1.2. Perumusan Masalah

Permasalahan pada penelitian ini adalah bagaimana menerapkan kombinasi metode *Vigenere Cipher* dan metode *Affine Cipher* untuk membuat dan memecahkan pesan rahasia.

1.3. Pembatasan Masalah

Pembatasan masalah dalam penelitian ini adalah:

1. Kunci sebanyak 4 kunci yang terdiri dari 2 kunci di metode *Vigenere Cipher* dan 2 kunci di metode *Affine Cipher*
2. Tanda baca (karakter) yang digunakan dibatasi pada 4 karakter yaitu \pm , $_$, $.$, $\%$.
3. Proses kombinasi diawali dengan metode *Vigenere Cipher* lalu menggunakan metode *Affine Cipher*.
4. Contoh penerapan terdiri dari 9 karakter, 24 karakter dan 58 karakter.

1.4. Tujuan

Tujuan yang diperoleh dari penelitian ini adalah dapat menerapkan kombinasi metode *Vigenere Cipher* dan metode *Affine Cipher*.

1.5. Manfaat

Manfaat yang diperoleh dari penelitian ini adalah:

1. Dapat menjadi rujukan pada mata kuliah terkait seperti aljabar linier terapan.
2. Dapat dijadikan referensi bagi penelitian lain.

DAFTAR PUSTAKA

- Anton, H. 1991. *Aljabar Linier Elementer*. Pantur Silaban Ph.D. (Penerjemah). Erlangga, Jakarta.
- Ariyus, D. 2008. *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*. Penerbit Andi, Yogyakarta.
- Hamdani. 2012, Penerapan Metode *Vigenere* Pada Kriptografi Klasik Untuk Pesan Rahasia. *Informatika Mulawarman*. Volume 7, No. 1.
- Irfan, M. Dwi Ramadhani. 2016. Perbandingan kriptografi klasik (caesar cipher) dan kriptografi modern (MD5). *Jurnal Teknik Informatika, Universitas Islam Sunan Gunung Djati*, Bandung.
- Juliadi, dkk. 2013. Kriptografi Klasik dengan Metode Modifikasi *Affine Cipher* yang Diperkuat dengan *Vigenere Cipher*. *Buletin Ilmiah Mat. Stat. dan Terapannya (Bilmaster)*. Vol. 02 No. 3 Hal. 87-92.
- Menezes, A., Van Oorschot, P. dan Vanstone, S. 2001. *Penerapan Ilmu Kriptografi*. Erlangga, Jakarta.
- Munir, R. 2006. *Kriptografi*, Informatika, Bandung.
- Philip, I. and Mario, G. 2006. A Modified Version of The *Vigenere* Algorithm. *Intenational Journal of Computer Science and Network Security*. Vol. 6 No. 3.
- Rorres, C. dan Anton, H. 2004. *Aljabar Linier Elementer Terapan*. Erlangga, Jakarta.
- Schneier, B. 1990. *Algoritma Metode-Metode Dalam Kriptografi*. Graham Ilmu, Yogyakarta.
- Septiarini, A. dan Hamdani. 2011, Sistem Kriptografi Untuk *Text Massage* Menggunakan Metode *Affine*. *Informatika Mulawarman*. Volume 7, No. 1.
- Sulasdianti. 2014. *Kriptografi dengan Kombinasi Metode Vigenere Cipher dan Metode Cipher Hill*. Universitas Sriwijaya. Indralaya.
- Steven, J.L. 1999. *Aljabar Linier dan Aplikasinya*. Erlangga, Jakarta.
- Vionita, A. dan Purboningsih, D. 2016. Penggunaan Metode Enkripsi *Vigenere* dan MD5 dalam Proses Pengamanan Pesan. *Seminar Nasional Matematika dan Pendidikan Matematika UNY 2016*. A-6.