

**PENYANDIAN PESAN DENGAN MENGGUNAKAN KRIPTOGRAFI  
HYBRID AUTOKEY VIGÈNERE CIPHER DAN ALGORITMA ELGAMAL**

**SKRIPSI**

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana  
Matematika



Oleh:

Anisa Nurul Hikmah

1607367

**DEPARTEMEN PENDIDIKAN MATEMATIKA  
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN  
ALAM UNIVERSITAS PENDIDIKAN INDONESIA  
2020**

## **LEMBAR HAK CIPTA**

### **PENYANDIAN PESAN DENGAN MENGGUNAKAN KRIPTOGRAFI HYBRID AUTOKEY VIGÈNERE CIPHER DAN ALGORITMA ELGAMAL**

Oleh:

Anisa Nurul Hikmah

NIM 1607367

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan

Alam

© Anisa Nurul Hikmah

Universitas Pendidikan Indonesia

Desember 2020

© Hak Cipta dilindungi undang-undang.

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian, dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

## LEMBAR PENGESAHAN

ANISA NURUL HIKMAH

### PENYANDIAN PESAN DENGAN MENGGUNAKAN KRIPTOGRAFI HYBRID AUTOKEY VIGENERE CIPHER DAN ALGORITMA ELGAMAL

Disetujui dan disahkan oleh pembimbing:

Pembimbing I



acc sidang

Dra. Hj. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II

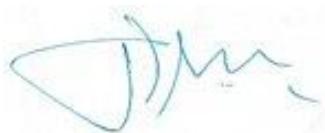


Husty Serviana Husain, S.Si. M.Si.

NIP. 198009182008122002

Mengetahui,

Ketua Departemen Pendidikan Matematika,



Dr. H. Dadang Juandi, M.Si.

NIP. 196401171992021001

## ABSTRAK

### “Penyandian Pesan dengan Menggunakan Kriptografi *Hybrid Autokey Vigènere Cipher* dan Algoritma El Gamal”

Seiring perkembangan teknologi, banyak cara yang dilakukan oleh peretas untuk menyadap pesan. Sehingga, keamanan data sangat diperlukan agar tidak terjadi kebocoran data. Salah satu cara agar data tidak diketahui oleh sembarang orang adalah dengan mengubahnya menjadi pesan tersamar. Ilmu yang mengajarkan pengubahan pesan menjadi pesan tersamar adalah kriptografi. Dalam penelitian ini, penulis mengkaji penyandian pesan dengan metode kriptografi *hybrid autokey Vigènere cipher* dan algoritma El Gamal. Algoritma *autokey Vigènere cipher* merupakan kriptografi simetris yang mana untuk proses enkripsi dan dekripsi nya serupa dengan *Vigènere cipher*, namun kekurangan kunci ditambahkan dari plainteksnya. Sedangkan, algoritma El Gamal merupakan kriptografi asimetris yang mana keamanannya terletak pada sulitnya memecahkan logaritma diskrit pada bilangan yang besar. Penulis memanfaatkan metode dua tingkatan kunci, di mana proses enkripsi dan dekripsi masing-masing dilakukan dua kali penguncian. Proses enkripsi menggunakan kunci rahasia *autokey Vigènere cipher* dan kunci publik El Gamal. Sedangkan, proses dekripsi menggunakan kunci privat El Gamal dan kunci rahasia *autokey Vigènere cipher*. Kriptografi *hybrid autokey Vigènere cipher* dan algoritma El Gamal ini memiliki tiga proses utama, yaitu pembangkitan kunci, enkripsi dan dekripsi. Konstruksi programnya menggunakan *Graphical User Interface (GUI)* dalam bahasa pemrograman python.

**Kata Kunci:** *Autokey Vigènere Cipher*, Dekripsi, El Gamal, Enkripsi, Kriptografi *Hybrid*

## ABSTRACT

### **“The Message Encoding Using Hybrid Autokey Vigènere Cipher Cryptography and El Gamal Algorithm”**

Since the technology has grown up, there are many ways the hackers can intercept messages. Thus, the data security is very necessary to prevent data leakage. To keep data safe from the people not authorized to access is by converting it into a cryptic message. The study of protecting messages into a cryptic message is cryptography. In this study, the researcher finds out the encryption of a messages using the hybrid Cryptography method autokey Vigènere cipher and El Gamal Algorithm. Autokey Vigènere Cipher algorithm is a symmetric cryptography which is the encryption and decryption processes using Vigènere cipher, however the plaintext is added to the keys to adding a lack of keys. While, El Gamal algorithm is an asymmetric cryptography which is the difficulty of solving discrete logarithms of large prime number used as a security of this algorithm. The researcher used a two-level key method, the encryption and decryption processes were each locked twice. The encryption process uses the Vigènere cipher's auto key secret key and the El Gamal public key. Meanwhile, the decryption process uses the El Gamal private key and the Vigènere Cipher auto key secret key. This hybrid cryptography Vigènere cipher and El Gamal algorithm has three main processes, there are key generation, encryption, and decryption. The implementation used the python programming language by utilizing a Graphical User Interface (GUI).

**Keywords:** *Autokey Vigènere Cipher, Decryption, El Gamal, Encryption, Hybrid Cryptography*

## DAFTAR ISI

### **LEMBAR PENGESAHAN**

### **LEMBAR PERNYATAAN KEASLIAN**

**KATA PENGANTAR**..... Error! Bookmark not defined.

**UCAPAN TERIMA KASIH**..... Error! Bookmark not defined.

**ABSTRAK**..... Error! Bookmark not defined.

**ABSTRACT** ..... Error! Bookmark not defined.

**DAFTAR ISI** ..... **vi**

**BAB 1 PENDAHULUAN**..... Error! Bookmark not defined.

    1.1 Latar Belakang Penelitian..... **Error! Bookmark not defined.**

    1.2 Rumusan Masalah ..... **Error! Bookmark not defined.**

    1.3 Batasan Masalah ..... **Error! Bookmark not defined.**

    1.4 Tujuan Penelitian ..... **Error! Bookmark not defined.**

    1.5 Manfaat Penelitian ..... **Error! Bookmark not defined.**

    1.6 Sistematika Penulisan..... **Error! Bookmark not defined.**

**BAB 2 LANDASAN TEORI**..... Error! Bookmark not defined.

    2.1 Landasan Matematika..... **Error! Bookmark not defined.**

        2.1.1 Bilangan Prima..... **Error! Bookmark not defined.**

        2.1.2 Pembagian..... **Error! Bookmark not defined.**

        2.1.3 Modular..... **Error! Bookmark not defined.**

        2.1.4 Invers Modular ..... **Error! Bookmark not defined.**

        2.1.5 Masalah Logaritma Diskrit ..... **Error! Bookmark not defined.**

    2.2 Kriptografi ..... **Error! Bookmark not defined.**

        2.2.1 Kriptografi Kunci Simetri..... **Error! Bookmark not defined.**

        2.2.2 Kriptografi Kunci Asimetris ..... **Error! Bookmark not defined.**

    2.3 Kriptosistem..... **Error! Bookmark not defined.**

        2.3.1 Vigènere *Cipher* ..... **Error! Bookmark not defined.**

- 2.3.2 Kriptanalisis Vigènere *Cipher* ..... **Error! Bookmark not defined.**
- 2.3.3 *Autokey* Vigènere *Cipher* ..... **Error! Bookmark not defined.**
- 2.3.4 Algoritma El Gamal ..... **Error! Bookmark not defined.**
- 2.3.5 Kriptografi *Hybrid* ..... **Error! Bookmark not defined.**
- 2.4 Bahasa Pemrograman Python ..... **Error! Bookmark not defined.**

### **BAB 3 METODOLOGI PENELITIAN** ..... Error! Bookmark not defined.

- 3.1. Mengidentifikasi Masalah ..... **Error! Bookmark not defined.**
- 3.2. Mengkaji Model Dasar ..... **Error! Bookmark not defined.**
- 3.3. Mengembangkan Model Dasar ..... **Error! Bookmark not defined.**
- 3.4. Mengkonstruksi Program ..... **Error! Bookmark not defined.**
  - 3.4.1 *Input* dan *Output* ..... **Error! Bookmark not defined.**
  - 3.4.2 Rancangan Tampilan Program Aplikasi ..... **Error! Bookmark not defined.**
  - 3.4.3 Algoritma Penyandian Pesan dengan Menggunakan Kriptografi *Hybrid Autokey Vigènere Cipher* dengan Algoritma El Gamal **Error! Bookmark not defined.**
- 3.5. Memvalidasi Program ..... **Error! Bookmark not defined.**
- 3.6. Kesimpulan ..... **Error! Bookmark not defined.**

### **BAB 4 HASIL PEMBAHASAN** ..... Error! Bookmark not defined.

- 4.1 Skema Penyandian Pesan Teks dengan Menggunakan Kriptografi *Hybrid Autokey Vigènere Cipher* dan Algoritma El Gamal ..... **Error! Bookmark not defined.**
- 4.2 Algoritma Penyandian Pesan Teks dengan Menggunakan Kriptografi *Hybrid Autokey Vigènere Cipher* dan Algoritma El Gamal ..... **Error! Bookmark not defined.**
- 4.3 Program Aplikasi Kriptografi *Hybrid Autokey Vigènere Cipher* dan Algoriitma El Gamal ..... **Error! Bookmark not defined.**
- 4.4 Validasi Program Aplikasi ..... **Error! Bookmark not defined.**

4.4.1	Contoh Pembangkitan Kunci Menggunakan Program Aplikasi Kriptografi <i>Hybrid Auto-Key Vigènere Cipher</i> dan Algoritma El Gamal.....	<b>Error! Bookmark not defined.</b>
4.4.2	Contoh Enkripsi Menggunakan Program Aplikasi Kriptografi <i>Hybrid AutoKey Vigènere Cipher</i> dan Algoritma El Gamal .....	<b>Error!</b>
4.4.3	Proses Enkripsi.....	<b>Error! Bookmark not defined.</b>
4.4.4	Contoh Dekripsi Menggunakan Program Aplikasi Kriptografi <i>Hybrid Autokey Vigènere Cipher</i> dan Algoritma El Gamal .....	<b>Error!</b>
4.4.5	Proses Dekripsi.....	<b>Error! Bookmark not defined.</b>
<b>BAB 5 KESIMPULAN DAN SARAN</b> .....		Error! Bookmark not defined.
5.1	Kesimpulan .....	<b>Error! Bookmark not defined.</b>
5.2	Saran.....	<b>Error! Bookmark not defined.</b>
<b>DAFTAR PUSTAKA</b> .....		<b>51</b>
<b>LAMPIRAN</b> .....		Error! Bookmark not defined.
<b>DAFTAR RIWAYAT HIDUP</b> .....		Error! Bookmark not defined.

## DAFTAR GAMBAR

- Gambar 2.1:** Skema Kriptografi Kunci Simetri ... **Error! Bookmark not defined.**
- Gambar 2.2:** Skema Kriptografi Kunci Publik .... **Error! Bookmark not defined.**
- Gambar 3.1:** Skema Kriptografi Autokey Vigènere *Cipher* **Error! Bookmark not defined.**
- Gambar 3.2:** Skema Algoritma El gamal..... **Error! Bookmark not defined.**
- Gambar 4.1:** Skema Pengamanan Pesan Menggunakan Kriptografi *Hybrid Autokey* Vigènère *Cipher* dan Algoritma El Gamal ..... **Error! Bookmark not defined.**
- Gambar 4.2:** Program Cek Bilangan Prima dangan GUI Python versi 3.8.3**Error! Bookmark not defined.**
- Gambar 4.3:** Program Pembangkitan Kunci dangan GUI Python versi 3.8.3 ..... **Error! Bookmark not defined.**
- Gambar 4.4:** Program Enkripsi dangan GUI Python versi 3.8.3**Error! Bookmark not defined.**
- Gambar 4.5:** Program Dekripsi dangan GUI Python versi 3.8.3 ..... **Error! Bookmark not defined.**
- Gambar 4.6:** Contoh Pembangkitan Kunci Menggunakan Program Aplikasi ..... **Error! Bookmark not defined.**
- Gambar 4.7:** Contoh Cek Bilangan Prima ..... **Error! Bookmark not defined.**
- Gambar 4.8:** Contoh Enkripsi Menggunakan Program Aplikasi ..... **Error! Bookmark not defined.**
- Gambar 4.9:** Contoh k *random* yang Dibangkitkan ..... **Error! Bookmark not defined.**
- Gambar 4.10:** Contoh Dekripsi Menggunakan Program Aplikasi ..... **Error! Bookmark not defined.**

## DAFTAR TABEL

**Tabel 4.1:** Tabel Enkripsi *Autokey Vigènere Cipher* ..... **Error! Bookmark not defined.**

**Tabel 4.2:** Tabel Enkripsi Algoritma El Gamal 1 . **Error! Bookmark not defined.**

**Tabel 4.3:** Tabel Enkripsi Algoritma El Gamal 2 . **Error! Bookmark not defined.**

**Tabel 4.4:** Tabel Dekripsi Algoritma El Gamal 1 . **Error! Bookmark not defined.**

**Tabel 4.5:** Tabel Dekripsi Algoritma El Gamal 2 . **Error! Bookmark not defined.**

**Tabel 4.6:** Tabel Dekripsi *Autokey Vigènere Cipher* ..... **Error! Bookmark not defined.**

## DAFTAR LAMPIRAN

- Lampiran 1.** Tabel ASCII ..... Error! Bookmark not defined.
- Lampiran 2.** Coding GUI Python untuk Program Cek Bilangan Prima ..... Error!  
Bookmark not defined.
- Lampiran 3.** Coding GUI Python untuk Program Pembangkitan Kunci.....Error!  
Bookmark not defined.
- Lampiran 4.** Coding GUI Python untuk Program Enkripsi Kriptografi *Hybrid Autokey Vigènere Cipher* dan Algoritma El Gamal .. Error! Bookmark not defined.
- Lampiran 5.** Coding GUI Python untuk Program Dekripsi Kriptografi *Hybrid Autokey Vigènere Cipher* dan Algoritma El Gamal .. Error! Bookmark not defined.
- Lampiran 6.** Perhitungan Kunci Publik y ..... Error! Bookmark not defined.
- Lampiran 7.** Perhitungan Enkripsi *Autokey Vigènere Cipher* Error! Bookmark not defined.
- Lampiran 8.** Perhitungan a (Cipherteks El Gamal) untuk Pembangkitan k  
*Random Pertama*..... Error! Bookmark not defined.
- Lampiran 9.** Perhitungan b (Cipherteks El Gamal) untuk Pembangkitan k  
*Random Pertama*..... Error! Bookmark not defined.
- Lampiran 10.** Perhitungan b (Cipherteks El Gamal) untuk Pembangkitan k  
*Random Kedua* ..... Error! Bookmark not defined.
- Lampiran 11.** Perhitungan m (Dekripsi El Gamal) untuk Pembangkitan k  
*Random Pertama*..... Error! Bookmark not defined.
- Lampiran 12.** Perhitungan m (Dekripsi El Gamal) untuk Pembangkitan k  
*Random Kedua* ..... Error! Bookmark not defined.
- Lampiran 13.** Perhitungan Dekripsi *Autokey Vigènere Cipher*... Error! Bookmark not defined.

## DAFTAR PUSTAKA

- Agrawal, A. dan Patankar, G. (2016). Design of Hybrid Cryptography Algorithm for Secure Communication. *International Research Journal of Engineering and Technology (IRJET)*, 3(1), 1323–1326.
- Amin, M. (2017). Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks. *Pseudocode*, 3(2), 129–136. doi: <https://doi.org/10.33369/pseudocode.3.2.129-136>.
- Ariska, Suroso dan Endri. (2018). Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher dan El Gamal pada Pengamanan Pesan Rahasia. Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri. *Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri (SENIATI)*, 328 – 336.
- Aulia, B.P. (2020). *Implementasi Hill Cipher pada Penyandian Gambar dengan Menggunakan Matlab*. (Skripsi). Sekolah Sarjana, Universitas Pendidikan Indonesia, Bandung.
- Basri. (2015). Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan). *Jurnal Ilmiah Ilmu Komputer*, 1(2), 31 – 36.
- Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*, 2(2), 18 – 23.
- Fangohr, H. (2004). *A Comparison of C, MATLAB and Python as Teaching Languages in Engineering*. doi: 10.1007/978-3-540-25944-2\_157
- Firdaus, J. (2017). *Penyandian Pesan Menggunakan Kombinasi Algoritma Rsa yang Ditingkatkan dan Algoritma Elgamal*. (Skripsi). Sekolah Sarjana, Universitas Pendidikan Indonesia, Bandung.

[Francis, N. dan Monoth, T. \(2018\).](#) An Analysis of Hybrid Cryptographic Approaches for Information Security *International Journal of Applied Engineering Research*, 13(3), 124–127.

Ifanto, M. (2009). Metode Enkripsi dan Dekripsi dengan Menggunakan Algoritma El Gamal. Makalah IF2091 Struktur Diskrit. Program Studi Informatika, Institut Teknologi Bandung.

[Jamaludin. \(2018\).](#) Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Jurnal dan Penelitian Teknik Informatika*. 2(2). 86 – 93.

Madhira, S dan Sammulal, P. (2014). Survey on Symmetric and Asymmetric Key Cryptosystems. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16(4), 11 – 18.

Menezes, A., Van Oorschot, P. dan Vanstone, S. (2001). *Handbook of applied cryptography*. CRC Press.

Munir, R. (2009). *Matematika Diskrit*. Bandung: Informatika.

Munir, R. (2018). Diktat Kuliah IF4020 Kriptografi. Program Studi Teknik Informatika, Institut Teknologi Bandung.

Munir, Rinaldi. (2019). Bahan Kuliah Pengantar Kriptografi. Program Studi Informatika, Institut Teknologi Bandung.

Pratiwi, L.E. (2014). *Program Aplikasi Kriptografi Penyandian One Time Pad Menggunakan Sandi Vigenere. (Skripsi)*. Sekolah Sarjana, Universitas Pendidikan Indonesia, Bandung.

Rejani, R., Deepu, V. dan Krishnan. (2015). Study of Symmetric key Cryptography Algorithms. *International Journal of Computer Techniques*, 2(2), 45–50.

- Reswan, Y dan Prabowo, D. A. (2018). Perancangan Aplikasi Pengamanan Data Text Menggunakan Kombinasi Algoritma Hill *Cipher* dan Algoritma RSA. *Jurnal Sistem Informasi (JSI)*, 10(2), 1535 – 1545.
- Rosen, K.H. (2012). *Discrete Mathematics and Its Applications, Seventh Edition*. New York: McGraw-Hill.
- Saraswat, A., Khatri, C., Sudhakar, Thakral, P., & Biswas, P. (2016). An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication. *Procedia Computer Science*, 92, 355-360. doi: <https://doi.org/10.1016/j.procs.2016.07.390>
- Schneier, Bruce. (1996). Applied Cryptography 2nd. John Wiley & Sons.
- Srinath, K.R. (2017). Python – The Fastest Growing Programming Language. . *International Research Journal of Engineering and Technology (IRJET)*, 4(12), 354 – 357.
- Stinson, D.R. (2006).Cryptography: theory and Practice Third Edition. Florida: CRC Press.
- Suguna, S., Dhanakoti, V. dan Manjupriya, R. (2016). A Study on Symmetric and Asymmetric Key Encryption Algorithms. *International Research Journal of Engineering and Technology (IRJET)*, 3(4), 27–31.
- Sutopo, S.F. (2020). *Implementasi Digital Signature Algorithm (Dsa) Menggunakan Secure Hash Algorithm-256 (Sha-256) pada Media Gambar*. (Skripsi). Sekolah Sarjana, Universitas Pendidikan Indonesia, Bandung.