# IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK PESAN RAHASIA BERBASIS WEB DI MARKAS PMI KOTA TANGERANG

**Rizky Fauzi**

Sistem Informasi, Universitas Pamulang
Jl. Raya Puspitek Serpong No. 10 Tangerang Selatan, Banten, Indonesia, 15310
E-mail: dosen08210@unpam.ac.id

**Abstrak**

Perkembangan teknologi dan ilmu pengetahuan pada era globalisasi ini semakin pesat dan canggih. Semua ini dikarenakan hasil dari pemikiran-pemikiran manusia yang semakin maju, hal tersebut dapat dilihat dari perkembangan ilmu komputer yang semakin hari semakin berkembang dengan pesat. Masalah yang sering terjadi di Markas PMI Kota Tangerang terkait komunikasi adalah terjadinya pelambatan pesan baik itu dalam hal menerima pesan ataupun memberikan pesan sehingga apabila ada sebuah permintaan atau tindakan sedikit terhambat untuk dilakukan. PMI Kota Tangerang mencoba melakukan terobosan dengan membuat program algoritma kriptografi elgamal. Berdasarkan permasalahan tersebut, maka dibuatlah sistem untuk mengirim pesan sesama karyawan dalam bentuk memo digital yang berfungsi agar pesan dapat disampaikan dengan cepat sehingga segala tindakan atau koordinasi dapat dilakukan sesuai dengan permintaan di memo. Dengan program ini staff atau pegawai dapat berkomunikasi dengan staff lain secara mudah dan cepat. Ketika ada permintaan pun tidak membutuhkan waktu lama untuk mengeksekusi atau mengerjakannya, dengan demikian pekerjaan dapat diselesakan dengan cepat..

Kata Kunci: Kriptografi, Elgamal, Pesan

## 1. PENDAHULUAN

Pengetahuan dan teknologi mejadi satu kesatuan di era globalisasi saat ini. Hal tersebut dapat dilihat dari perkembangan ilmu komputer yang semakin berkembang dengan pesat. Selain itu, perkembangan teknologi semakin mendukung untuk penyebaran informasi melalui media cetak di seluruh lapisan masyarakat. Penyebaran informasi tidak hanya bisa diperoleh melalui media cetak saja tetapi bisa juga didapatkan melalui media elektronik seperti televisi, radio, dan internet.

Informasi adalah data yang telah diolah menjadi sebuah bentuk yang berarti bagi penerimanya dan bermanfaat dalam mengambil keputusan saat ini atau mendatang (Agustin, 2018). Berkembangnya teknologi informasi berbasis komputer memudahkan organisasi atau perusahaan melakukan aktivitas mengakses informasi dimana dan kapan saja. Dalam hubungannya dengan aktivitas yang terjadi pada setiap hari pada perusahaan, terutama pada aktivitas yang ditujukan menghasilkan produk dan jasa, teknologi informasi membantu menciptakan produk yang sangat kompetitif.

Kecanggihan teknologi informasi bila diaplikasikan pada rantai aktivitas akan menghasilkan produk Untuk menunjang efektifias, produktifitas dan efisiensi sebuah sistem manajemen dalam sebuah instansi/perusahaan maka perlu adanya sistem komputerisasi yang baik dan berdaya guna. PMI Kota Tangerang sedang mencoba menerapkan sistem komputerisasi yang baik dan berdaya guna. Terobosan baru ini akan menjadi *pioneer* untuk sistem-sistem lainnya. Sistem yang akan dibuat adalah Pengiriman pesan antar karyawan dengan komputerisasi. Dengan adanya sistem ini, akan menguruangi penggunaan kertas bahkan lebih mempercepat penyampaian pesan antar karyawan.

Sistem pengiriman pesan ini bertujuan untuk menciptakan kinerja yang efektif dan efisien agar lebih mudah untuk menyampaikan informasi yang bersifat urgent/mendadak sehingga tidak banyak waktu dan biaya yang terbuang. Salah satu aspek sistem ini adalah peningkatan komunikasi antar karyawan apabila ingin berkomunikasi dengan jarak jauh.

Permasalahan yang sering terjadi adalah dalam proses penyampaian pesan singkat

(memo) ini sering kali pelambatan dalam hal penerimaan pesan sehingga apabila ada permintaan terlambat untuk dilaksanakan. Biasanya, pesan singkat yang ingin disampaikan harus dicetak sehingga selalu harus melakukan beberapa proses, dimulai dari pengetikan, pencetakan hingga pengiriman pesan. Hal ini disebabkan sistem ini belum ada. Ketika sistem ini terbentuk, pegawai tidak perlu lagi untuk mencetak pesan dan mengirimkan pesan tersebut.

## 2. LANDASAN TEORI

Landasan teori dalam penelitian ini mengutip beberapa penelitian terdahulu yang telah dipublikasi dalam bentuk jurnal untuk di jadikan referensi pengembangan sistem informasi yang akan dijabarkan dalam penelitian ini.

### Implementasi

Implementasi merupakan suatu proses mendapatkan suatu hasil yang sesuai dengan tujuan atau sasaran kebijakan itu sendiri. Dimana pelaksana kebijakan melakukan suatu aktivitas atau kegiatan (Irawan & Simargolang, 2018).

### Algoritma

Algoritma adalah urutan aksi-aksi yang dinyatakan dengan jelas dan tidak rancu untuk memecahkan suatu masalah dalam rentang waktu tertentu. Setiap aksi harus dapat dikerjakan dan mempunyai efek tertentu. Algoritma merupakan logika, metode dan tahapan (urutan) sistematis yang digunakan untuk memecahkan suatu permasalahan (Jodi, 2020).

### Kriptografi

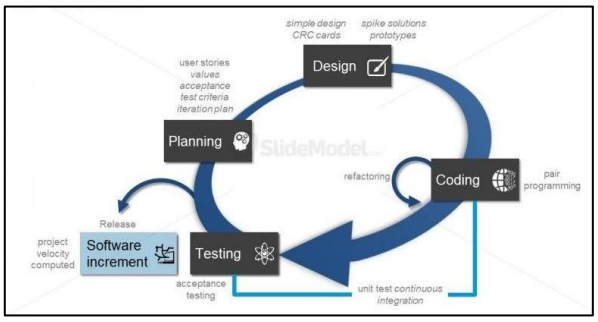
Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematikauntuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas (Nurhasan, 2019). Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

### Algoritma Elgamal

Algoritma ElGamal dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada mulanya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan dekripsi. Algoritma ElGamal merupakan jenis algoritma asimetris karena menggunakan kunci yang berbeda untuk proses enkripsi dan proses dekripsi (Hendrawaty et al., 2022).

## 3. METODE PENELITIAN

Dalam penelitian ini, implementasi algoritma elgamal di PMI Kota Tangerang menggunakan metode *Extreme Programming* atau biasa juga dikenal dengan XP method. *Extreme Programming* ini merupakan merupakan metodologi yang digunakan untuk pengembangan perangkat lunak yang ditujukan dalam meningkatkan kualitas perangkat lunak terhadap perubahan serta kebutuhan pelanggan. Pada pengembangan ini jenis perangkat lunak dimaksudkan untuk meningkatkan produktivitas dan memperkenalkan pos pemeriksaan yang mana persyaratan pelanggan baru dapat (Ariyanti et al., 2020).




**Gambar 3.1 Alur Tahapan *Extreme Programming***

Pada metode *Extreme Programming* terdapat empat tahapan utama dimana keempat tahapan ini berfokus pada tahap ketiga yakni penulisan kode atau *coding*. Adapun tahapan-tahapn tersebut, antara (Borman et al., 2020):

a. *Planning* atau Perencanaan
   Pada tahap ini, dilakukan sebuah perencanaan terhadap sistem yang akan dibangun. Tahap ini diawali dengan pemahaman alur dan proses bisnis seperti penggambaran sistem yang sedang berjalan, sistem yang dibutuhkan, kapasitas dan batasan sistem yang dikembangkan serta tahapan kemajuan.
b. *Design* atau Perancangan
   Pada tahap ini dilakukan pembuatan model sistem yang biasanya dibuat dalam bentuk diagram. Dalam penelitian ini visualisasi diagram dengan menggunakan *usecase diagram*, *activity diagram, sequence diagram, class diagram* dan *entity relationship diagram* yang mana masing-masing diagram mewakili proses pengembangan sistem.
c. *Coding* atau Pengkodean
   Pada tahapan ini dilakukan penulisan kode dengan bahasa pemrograman yang ditentukan berdasarkan model yang telah divisualisasikan sebelumnya pada tahapan perancangan.

Dalam penelitian ini digunakan bahasa PHP sebagai bahasa pemrograman untuk *back-end*. Dalam proses penyimpanan data sistem ini akan menggunakan database yang dibangun dengan MySQL.

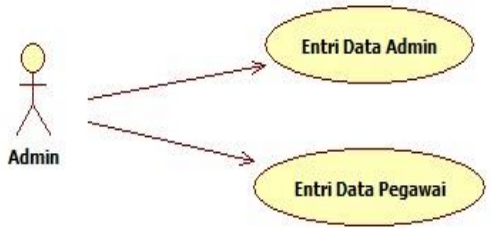
d. *Testing* atau Pengujian
Pada tahapan ini dilakukan proses pengujian sistem yang telah dibuat sebelumnya. Dalam penelitian ini, pengujian sistem dilakukan dengan metode *black-box* dan *white-box*.

## 4. HASIL DAN PEMBAHASAN

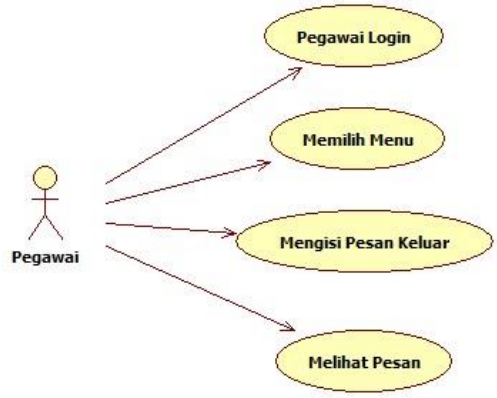
Proses pengembangan sistem pesan rahasia dengan metode *extreme programming* diawali dengan penentuan masalah dan menganalisa kebutuhan instansi. Analisa kebutuhan dilakukan dengan membuat *use case diagram*, *activity diagram, sequence diagram* dan *class diagram* yang biasa dikenal dengan *Unified Modelling Language* atau disingkat UML. UML (Unified Modeling Language) adalah sebuah bahasa yang berdasarkan grafik/gambar untuk memvisualisasi, menspesifikasikan, membangun, dan pendokumentasian dari sebuah sistem pengembangan software berbasis OO (Object-Oriented). UML sendiri juga memberikan standar penulisan sebuah sistem blue print, yang meliputi konsep bisnis proses, penulisan kelas-kelas dalam bahasa program yang spesifik, skema database, dan komponen-komponen yang diperlukan dalam sistem software (Mubarak & Metro, n.d.). Sistem ini dikembangkan untuk digunakan oleh dua pengguna, yakni admin dan staff/pegawai.

### *Use Case Diagram*

Use case diagram menggambarkan secara grafis perilaku software aplikasi. Adapun use case diagram dibawah ini adalah Implementasi Algoritma Kriptografi Elgamal untuk Peasn Rahasia di Markas PMI Kota Tangerang. Berikut adalah penggambaran *use case diagram* untuk sistem pesan rahasia dalam penelitian ini.



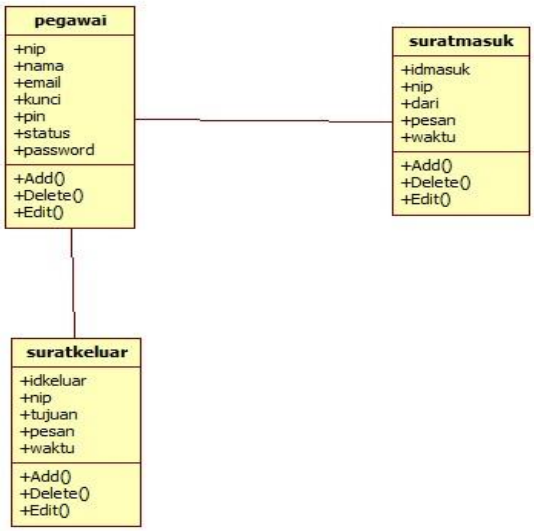

**Gambar 4.1 *Use Case Diagram* Admin**




**Gambar 4.2 *Use Case Diagram* Pegawai**

### *Class Diagram*

Selanjutnya adalah membuat *class diagram* untuk menjabarkan bagian-bagian sistem berdasarkan kelas yang telah direncanakan. Berikut *class diagram* dalam sistem dalam penelitian ini:



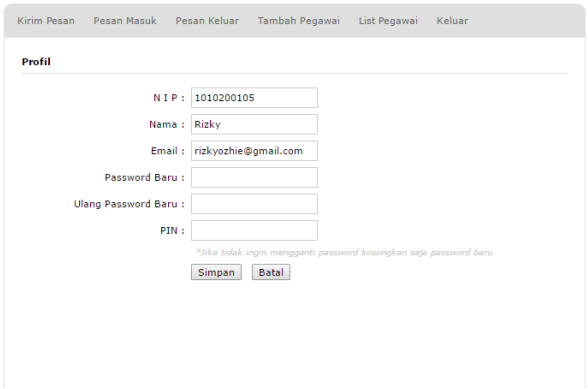

**Gambar 4.3 *Class Diagram***

### Pengujian *Black Box*

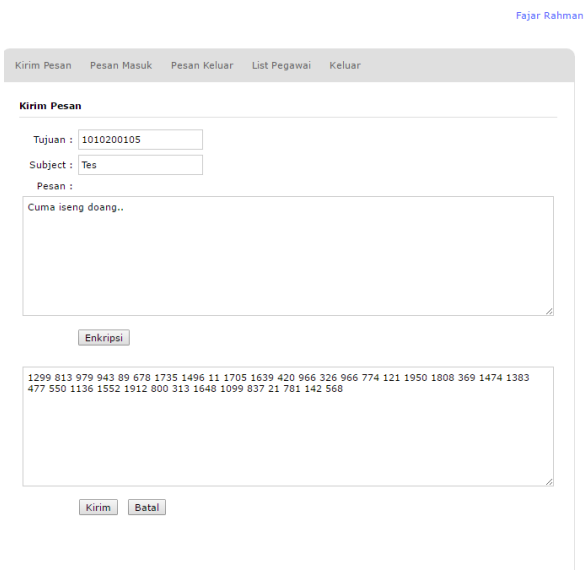
Salah satu metode pengujian yang berfokus pada spesifikasi fungsionalitas dari perangkat lunak disebut Black Box Testing. Teknik pengujian Black Box yaitu pengujian yang dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak. Jadi dianalogikan seperti kita melihat suatu kotak hitam, kita hanya bisa melihat penampilan luarnya saja, tanpa tahu ada apa dibalik bungkus hitam nya. Sama seperti pengujian black box, mengevaluasi hanya dari tampilan luarnya (interface), fungsionalitasnya tanpa mengetahui apa sesungguhnya yang terjadi dalam proses detilnya (Astuti, 2018).


**Gambar 4.4 Halaman *Login***


**Gambar 4.5 Dashboard Pegawai**

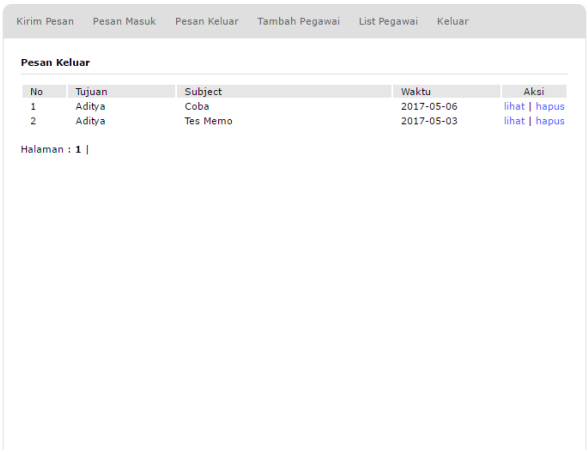



**Gambar 4.6 Halaman Profil Pegawai**

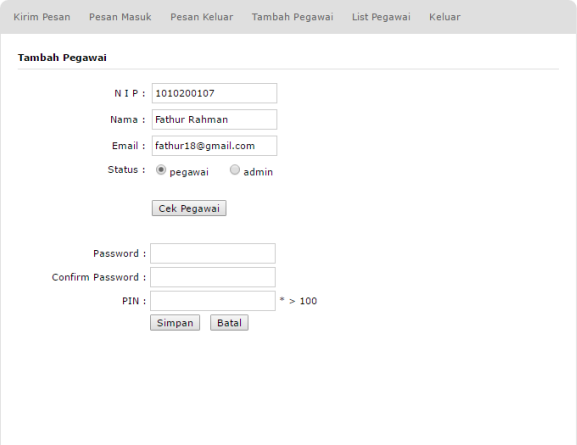



**Gambar 4.7 Halaman Kirim Pesan**


**Gambar 4.8 Halaman Pesan Masuk**




**Gambar 4.9 Halaman Pesan Keluar**




**Gambar 4.10 Halaman Tambah Pegawai**

| Kasus/Proses | Hasil |
|---|---|
| **Halaman Login**<br>NIP : 02810<br>Password : 54321<br>Pin : 111 | Berhasil login |
| **Halaman Profil Pegawai**<br>Klik nama user | Muncul tampilan profil pegawai |
| **Pesan Masuk**<br>Pilih menu pesan masuk | Muncul tampilan pesan masuk |
| **Pesan Keluar**<br>Pilih menu pesan keluar | Muncul tampilan pesan keluar |
| **Kirim Pesan**<br>Input<br>Tujuan: 1010200105<br>Subjek: Tes<br>Pesan: Cuma iseng doang<br>Klik tombol ekripsi | Pesan berhasil disimpan |
| **Tambah Pegawai**<br>Input<br>NIP: 1010200107<br>Nama: Fathur Rahman<br>Email: fathur10@gmail.com<br>Status: pegawai<br>Password:123456<br>Confirm Password: 123456 | Data Berhasil disimpan |

## 5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

a. Aplikasi yang dibuat dapat mempercepat komunikasi antar staff/pegawai Markas PMI Kota Tangerang melalui pesan rahasia.
b. Tampilan (*interface*) aplikasi yang dibuat masih sederhana, perlu adanya pengembangan yang lebih baik.
c. Untuk saat ini, aplikasi tersebut tidak dapat digunakan lagi karena sudah banyak aplikasi yang lebih baik untuk berkomunikasi seperti: WhatsApp, Facebook dan lain-lain.

## DAFTAR PUSTAKA


Agustin, H. (2018). Sistem informasi manajemen menurut prespektif islam. *Jurnal Tabarru': Islamic Banking and Finance*, *1*(1), 63–70.

Ariyanti, L., Satria, M. N. D., & Alita, D. (2020). Sistem Informasi Akademik Dan Administrasi Dengan Metode Extreme Programming Pada Lembaga Kursus Dan Pelatihan. *Jurnal Teknologi Dan Sistem Informasi*, *1*(1), 90–96.

Astuti, P. (2018). Penggunaan Metode Black Box Testing (Boundary Value Analysis) Pada Sistem Akademik (Sma/Smk). *Faktor Exacta*, *11*(2), 186–195.

Borman, R. I., Priandika, A. T., & Edison, A. R. (2020). Implementasi Metode Pengembangan Sistem Extreme Programming (XP) pada Aplikasi Investasi Peternakan. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *8*(3), 272–277.

Hendrawaty, H., TB, D. R. Y., & Munawir, M. (2022). ANALISIS HASIL ENKRIPSI DAN DEKRIPSI CITRA RGB 24 BIT MENGGUNAKAN ALGORITMA ELGAMAL BERDASARKAN UKURAN, DAN WARNA CITRA ASLI. *JOURNAL OF INFORMATICS AND COMPUTER SCIENCE*, *8*(1), 12–16.

Irawan, M. D., & Simargolang, S. A. (2018). Implementasi E-Arsip pada program studi teknik informatika. *(JurTI) Jurnal Teknologi Informasi*, *2*(1), 67–84.

Jodi, M. R. D. (2020). *Algoritma dan Struktur data*.

Mubarak, A., & Metro, J. J. (n.d.). *RANCANG BANGUN APLIKASI WEB SEKOLAH MENGGUNAKAN UML (UNIFIED MODELING LANGUAGE) DAN BAHASA PEMROGRAMAN PHP (PHP HYPERTEXT PREPROCESSOR) BERORIENTASI OBJEK*.

Nurhasan, A. (2019). Perancangan Sistem Keamanan Data Inventory Barang Di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Cipher. *Jurnal Teknologi Informasi MURA*, *11*(01), 29–36.