

Diagnosa Tumor Otak Berdasarkan Citra MRI (Magnetic Resonance Imaging), *Ida Bagus Leo Mahadya Suta, Rukmi Sari Hartati, Yoga Divayana*

Analisis Metode Sistem Pendukung Keputusan Pemilihan Waktu Terbaik Perubahan Harga Dinamis Hotel, *I Wayan Surya Pramana, Rukmi Sari Hartati, Yoga Divayana*

Penerapan Metode Forward Chaining Untuk Rekomendasi Instalasi Local Area Network (LAN) Menggunakan Pengujian System Usability Scale (SUS), *I Wayan Surya Pramana, Lie Jasa*

Evaluasi Infrastruktur Jaringan LAN OPD Pemerintah Provinsi Bali dengan COBIT 5.0, *Antara, G.M.B, Linawati, Wirastuti, NMAE.D*

Penentuan Harga Jual Biji Jarak Kering Dengan Metode Activity Based Cost System Untuk Mendukung Pertanian Berkelanjutan: Studi Kasus Nusa Penida, Bali, *Radha Kurniawan, Rukmi Sari Hartati, I N Satya Kumara*

Simulasi Filter Aktif pada 6 Pulse STATCOM Untuk Mereduksi Total Harmonic Distortion (THD) Di Sistem Transmisi Bali, *Made Dika Nugraha, Ida Bagus Gede Manuaba, Rukmi Sari Hartati*

Sistem Pengamanan Anonym dengan Menggunakan Algoritma Kriptografi ElGamal, *Ni Komang Ayu Sri Anggreni, Linawati, I Nyoman Putra Sastra*

Studi Manajemen Energi Listrik di RSUD Kabupaten Klungkung, *I Nyoman Yudiyana, I Nyoman Satya Kumara, Rukmi Sari Hartati*

Pemanfaatan Autotransformator Sebagai Pengontro Arus Start Motor Induksi Tipe LH 73204 Guna Menjaga Kesetabilan Tegangan Listrik di Laboratorium Konversi Energi Teknik Elektro Universitas Udayana, *I Wayan Lastera*

Analisa Pengaruh Jarak Sudu Terhadap Putaran Turbin Ulir Pada Pembangkit Listrik Tenaga Mikro Hidro, *I Kadek Agus Ardika, Antonius Ibi Weking, Lie Jasa*

Analisa Sentiment Untuk Opini Alumni Perguruan Tinggi, *I Komang Dharmendra, Komang Oka Saputra, Nyoman Pramaita*

Analisis Kualitas Citra Medis Terkopresi JPEG, *Derry Suia, Oka Widyantara, Rukmi Hartati*

Peramalan Penerbitan Ijin Mendirikan Bangunan Dengan Single Moving Average Dan Exponential Smoothing, *I Gst. Ngr. Agung Yogha P, Rukmi Sari Hartati, Komang Oka Saputra*

Analisa Kualitas Daya Listrik Instalasi Wing Amerta RSUP Sanglah Denpasar, *I Putu Meyyasa, Rukmi Sari Hartati, I.B. Gede Manuaba*

Evaluasi Kualitas Dan Kepuasan Pengguna Website Imissu Dengan Penerapan Metode Webqual 4.0, *I Ketut Citra Adi Putra, Komang Oka Saputra, Wayan Gede Ariastina*

Studi Pengelolaan Model Manajemen Pemeliharaan Garpu Tala di PT PLN (Persero) Unit Pelaksana Pelayanan Pelanggan (UP3) Bali Timur, *Dewa Ayu Nancy Cahyani, Rukmi Sari Hartati, Wayan Gde Ariastina*

Analisis Perbandingan Routing Protocol Open Shortes Path First dan Enhanced Interior Gateway Routing Protocol pada IPV6 menggunakan Graphical Network Simulator 3, *Made Dinda Pradnya Pramita, Lie Jasa*

Deteksi Tipe Modulasi Digital Pada Automatic Modulation Recognition Menggunakan Support Vector Machine dan Conjugate Gradient Polak Ribiere-Backpropagation, *Ni Luh Komang Tri Wahyuni M.U, I Made Oka Widyantara, Ni Made Ary Esta Dewi W*

Penerapan Teknologi Informasi dalam Reformasi Birokrasi pada Bidang Pendidikan, *Anak Agung Made Dian Krisnandari, Dewa Made Wiharta, Nyoman Putra Sastra*

Analisis Retrofit Lampu Di Kantor Wilayah BRI Denpasar Dengan Metode Life Cycle Cost, *Muhammad Hari Wijaya, Rukmi Sari Hartati, Wayan Gede Ariastina*



# **SUSUNAN DEWAN REDAKSI**

## **MAJALAH ILMIAH TEKNOLOGI ELEKTRO**

### **Penanggung Jawab**

Prof. Ir. Ngakan Putu Gede Suardana, MT. PhD.

### **Advisory Board**

Ir. Linawati, M.Eng, M.Eng.Sc, Ph.D.

### **Editor-in-Chief**

Dr. Ir. Lie Jasa, MT.

### **Editorial Board**

Prof. I. A. Giriantari, Ph.D.(UNUD) (Scopus ID : 6507145301)| Dr. Ingrid Nurtanio (UNHAS) (Scopus ID: 55746722900)|Yoga Divayana, Ph.D.(UNUD) (Scopus ID: 8979718500)|Dr. Made Ginarsa (UNRAM) (Scopus ID: 35795378400)|Dr. Iwan setiawan (UNDIP) (Scopus ID : 56711777600)|Linawati, Ph.D.(UNUD) (Scopus ID: 52763653600)

### **Reviewer**

Prof. Rukmi Sari Hartati, Ph.D.(UNUD) (Scopus ID: 6508088351)| Prof. I Ketut Gede Darma Putra. (UNUD) (Scopus ID: 55847371700) | Setyawan Sakti Purnomo,Ph.D. (UB) (Scopus ID: 6507450797) | WG Ariastina, PhD. (UNUD) (Scopus ID: 6507932528) |Dr. Dian Sawitri (UDINUS) (Scopus ID: 35796192800) | Dr. Ratna Ika Putri (POLINEMA) (Scopus ID: 46461783800) | Dr. Kalvein Rantelobo (UNDANA) (Scopus ID: 35796140100) | I N Satya Kumara, Ph.D. (UNUD) (Scopus ID: 55913974900) | Dr. Moch. Arief Soeleman (UDINUS) (Scopus ID: 55598790600) | Dr. Radi (UGM) (Scopus ID: 56916103300) |Dr. Oka Widyantara (UNUD) (Scopus ID: 54897989200) |Dr. Lilik Anifah (UNESA) (Scopus ID: 55648855000) | Dr. Dewa Made Wiharta (UNUD) (Scopus ID: 57092646100) | Dr. Ruri Suko Basuki (UDINUS) (Scopus ID: 56622972000) | Dr. Nyoman Putra Sastra (UNUD) (Scopus ID: 24767212900) | Dr. Nyoman Sukajaya (GANESHA) (Scopus ID: 57200412316) | Dr. Made Sudarma (UNUD) (Scopus ID: 6506568234)|Dr. Ramadoni Syahputra (UMY) (Scopus ID: 55331465900) | N.M.A.E.D. Wirastuti, Ph.D.(UNUD) (Scopus ID: 24722146300) | Dr. Purwoharjono (UNTAN) (Scopus ID: 55001864700) | Komang Oka Saputra.Ph.D. (UNUD) (Scopus ID: 57024177000) | Dr. Alit Swamardika (UNUD) (Scopus ID: 56021560800) | Nyoman Pramaita, Ph.D.(UNUD) (Scopus ID: 57193931092) | Sukerayasa (UNUD) (Scopus ID: 56123138400) | Cahyo Durujati (NAROTAMA) (Scopus ID: 56027926800) | Nyoman Setiawan (UNUD)(Scopus IID: 57193929655)

**Alamat Redaksi**  
**PROGRAM STUDI MAGISTER**  
**TEKNIK ELEKTRO**

Universitas Udayana Bali

email :

jteudayana@gmail.com | miteudayana@gmail.com | liejasa@unud.ac.id

Telp./Fax : 0361 239599

Di Index oleh :

**Google Scholar | IPI | DOAJ | EBSCO | One Search | Base | OAJI**  
**| ARI | SHERPA/RoMEO | JournalTOCs | Sinta**

Anggota dari :

**Turnitin | Crossref**

**Peringkat Akreditasi Sinta 3**

berdasarkan Surat Keputusan Direktur Jenderal Penguatan Riset dan Pengembangan  
Kemristekdikti No. 28 / E / KPT / 2019, tanggal 26 September 2019

MAJALAH ILMIAH  
**TEKNOLOGI ELEKTRO**

Vol. 18 No. 2 Mei – Agustus 2019

P-ISSN : 1693-2951, e-ISSN : 2503-2372

---

Diagnosa Tumor Otak Berdasarkan Citra MRI ( <i>Magnetic Resonance Imaging</i> ), <i>Ida Bagus Leo Mahadya Suta, Rukmi Sari Hartati, Yoga Divayana</i> .....	149-154
Analisis Metode Sistem Pendukung Keputusan Pemilihan Waktu Terbaik Perubahan Harga Dinamis Hotel, <i>I Wayan Surya Pramana, Rukmi Sari Hartati, Yoga Divayana</i> .....	155-164
Penerapan Metode Forward Chaining Untuk Rekomendasi Instalasi Local Area Network (LAN) Menggunakan Pengujian System Usability Scale (SUS), <i>I Wayan Surya Pramana, Lie Jasa</i> .....	165-172
Evaluasi Infrastruktur Jaringan LAN OPD Pemerintah Provinsi Bali dengan COBIT 5.0, <i>Antara, G.M.B, Linawati, Wirastuti, NMAE.D</i> .....	173-180
Penentuan Harga Jual Biji Jarak Kering Dengan Metode Activity Based Cost System Untuk Mendukung Pertanian Berkelanjutan: Studi Kasus Nusa Penida, Bali, <i>Radha Kurniawan, Rukmi Sari Hartati, I N Satya Kumara</i> .....	181-190
Simulasi Filter Aktif pada 6 Pulse STATCOM Untuk Mereduksi Total Harmonic Distortion (THD) Di Sistem Transmisi Bali, <i>Made Dika Nugraha, Ida Bagus Gede Manuaba, Rukmi Sari Hartati</i> .....	191-196
Sistem Pengamanan Anonym dengan Menggunakan Algoritma Kriptografi ElGamal, <i>Ni Komang Ayu Sri Anggreni, Linawati, I Nyoman Putra Sastra</i> .....	197-202
Studi Manajemen Energi Listrik di RSUD Kabupaten Klungkung, <i>I Nyoman Yudiyana, I Nyoman Satya Kumara, Rukmi Sari Hartati</i> .....	203-210
Pemanfaatan Autotransformator Sebagai Pengontro Arus Start Motor Induksi Tipe LH 73204 Guna Menjaga Kesetabilan Tegangan Listrik di Laboratorium Konversi Energi Teknik Elektro Universitas Udayana, <i>I Wayan Lastera</i> .....	211-216

Analisa Pengaruh Jarak Sudu Terhadap Putaran Turbin Ulir Pada Pembangkit Listrik Tenaga Mikro Hidro, <i>I Kadek Agus Ardika, Antonius Ibi Weking, Lie Jasa</i> .....	217-226
Analisa Sentiment Untuk Opini Alumni Perguruan Tinggi, <i>I Komang Dharmendra, Komang Oka Saputra, Nyoman Pramaita</i> .....	227-234
Analisis Kualitas Citra Medis Terkopresi JPEG, <i>Derry Suia, Oka Widyantara, Rukmi Hartati</i> .....	235-240
Peramalan Penerbitan Ijin Mendirikan Bangunan Dengan Single Moving Average Dan Exponential Smoothing, <i>I Gst. Ngr. Agung Yogha P, Rukmi Sari Hartati, Komang Oka Saputra</i> .....	241-248
Analisa Kualitas Daya Listrik Instalasi Wing Amerta RSUP Sanglah Denpasar, <i>I Putu Meyyasa, Rukmi Sari Hartati, I.B. Gede Manuaba</i> .....	249-258
Evaluasi Kualitas Dan Kepuasan Pengguna Website Imissu Dengan Penerapan Metode Webqual 4.0, <i>I Ketut Citra Adi Putra, Komang Oka Saputra, Wayan Gede Ariastina</i> .....	259-266
Studi Pengelolaan Model Manajemen Pemeliharaan Garpu Tala di PT PLN (Persero) Unit Pelaksana Pelayanan Pelanggan (UP3) <i>Bali Timur, Dewa Ayu Nancy Cahyani, Rukmi Sari Hartati, Wayan Gde Ariastina</i> .....	267-274
Analisis Perbandingan Routing Protocol Open Shortes Path First dan Enhanced Interior Gateway Routing Protocol pada IPV6 menggunakan Graphical Network Simulator 3, <i>Made Dinda Pradnya Pramita, Lie Jasa</i> .....	275-280
Deteksi Tipe Modulasi Digital Pada Automatic Modulation Recognition Menggunakan Support Vector Machine dan Conjugate Gradient Polak Ribiere-Backpropagation, <i>Ni Luh Komang Tri Wahyuni M.U, I Made Oka Widyantara, Ni Made Ary Esta Dewi W</i> .....	281-286
Penerapan Teknologi Informasi dalam Reformasi Birokrasi pada Bidang Pendidikan, <i>Anak Agung Made Dian Krisnandari, Dewa Made Wiharta, Nyoman Putra Sastra</i> .....	287-292
Analisis Retrofit Lampu Di Kantor Wilayah BRI Denpasar Dengan Metode Life Cycle Cost, <i>Muhammad Hari Wijaya, Rukmi Sari Hartati, Wayan Gede Ariastina</i> .....	293-298

# Sistem Pengamanan *Anonym* dengan Menggunakan Algoritma Kriptografi ElGamal

Ni Komang Ayu Sri Anggreni<sup>1</sup>, Linawati<sup>2</sup>, I Nyoman Putra Sastra<sup>3</sup>

[Submission: 20-04-2019, Accepted: 30-06-2019]

**Abstract**— Reporting on act of domestic violence to Integrated Services Center for Woman and Children (Pusat Pelayanan Terpadu Pemberdayaan Perempuan dan Anak (P2TP2A)) Denpasar City is kind of sensitive and vulnerable data to tapping. As a result, security guarantee for the reporter is needed to protect their identity. Security guarantee with anonym reporting system, which uses ElGamal cryptographic algorithm for encryption process and description process. ElGamal cryptographic algorithm is one of asymmetric cryptography which consist of 3 processes, that are process of generate key, encryption process and description process. On this security system identity of the reporter will be protected through process of authentication, authorization, and encryption. In this study the researcher uses Android platform and ElGamal cryptographic algorithm for encryption and description, Firebase Auth for authentication, Firebase Rules for authorization and Avalanche Effect for knowing the quality of cryptographic algorithm. The result of the trials which used 10 different cipher texts of avalanche effect is 58,2%. That result can be categorized as good because a good result of avalanche effect.

**Intisari**— Pelaporan tindak kekerasan rumah tangga pada Pusat Pelayanan Terpadu Pemberdayaan Perempuan dan Anak (P2TP2A) Kota Denpasar merupakan data yg sensitive dan rawan terhadap penyadapan. Maka dari itu diperlukan jaminan keamanan kepada pelapor pengaduan agar identitasnya dapat dilindungi. Jaminan keamanan yang dimaksud adalah sistem pelaporan tindak kekerasan dengan pengamanan yang anonym, menggunakan algoritma kriptografi ElGamal untuk proses enkripsi dan proses dekripsi. Algoritma kriptografi ElGamal merupakan salah satu jenis kriptografi asimetris dimana terdiri dari tiga proses yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Pada sistem pengamanan ini identitas pelapor dijaga kerahasiaannya dan terbukti kebenarannya melalui proses autentikasi, otorisasi, dan enkripsi. Dalam studi ini menggunakan platform Android dan algoritma kriptografi ElGamal untuk enkripsi dan dekripsi, Firebase Auth untuk autentikasi, Firebase Rules untuk otorisasi serta Avalanche Effect untuk mengetahui baik tidaknya algoritma kriptografi. Dari hasil uji coba dengan menggunakan 10 cipher text yang berbeda diketahui bahwa hasil perhitungan avalanche effect yang dihasilkan rata-rata 58,2 %. Hasil tersebut dikatakan baik mengingat avalanche effect dikategorikan baik apabila berkisar antara 40-60%.

**Kata Kunci**—Kriptografi, Enkripsi, Android, ElGamal

## I. PENDAHULUAN

Saat ini perkembangan teknologi informasi salah satunya internet sangatlah berpengaruh hampir pada seluruh aspek kehidupan manusia termasuk dalam berkomunikasi. Namun, banyak terjadi penyadapan informasi yang dilakukan oleh pihak yang tidak bertanggung jawab sehingga menyebabkan internet tidaklah terlalu aman. Karena banyaknya yang menggunakan internet, maka perlu dipikirkan untuk memberikan jaminan keamanan pada data yang *sensitive*, terutama data yang hanya bisa diketahui oleh pihak tertentu saja.

Salah satu contoh sistem yang mempunyai data *sensitive* adalah pada pelaporan tindak kekerasan pada Pusat Pelayanan Terpadu Pemberdayaan Perempuan dan Anak (P2TP2A) Kota Denpasar. Pelapor pengaduan pada sistem ini diberikan jaminan keamanan agar identitasnya dapat dilindungi. Jaminan keamanan yang dimaksud adalah sistem pelaporan tindak kekerasan dengan pengamanan yang *anonym*, menggunakan algoritma kriptografi untuk proses enkripsi dan proses dekripsi [1]. Dalam sistem pelaporan ini akan dilakukan sedikit pengembangan dengan menggunakan metode algoritma kriptografi ElGamal.

*Ciphertext* yang dihasilkan oleh algoritma ElGamal akan selalu berbeda meskipun menggunakan kunci dan pesan yang sama sehingga hal tersebut merupakan keunggulan daripada algoritma ElGamal sehingga tingkat keamanan yang dihasilkan lebih tinggi. Hal tersebut membuat jumlah karakter *chiphertext* yang dihasilkan lebih banyak sehingga membutuhkan waktu yang lama apabila sistem akan di retas serta kecepatan waktu proses enkripsi dan dekripsi akan menjadi lebih lambat [2].

Dibandingkan dengan algoritma asimetris lainnya, algoritma kriptografi ElGamal lebih aman karena menghasilkan *ciphertext* lebih kompleks sehingga membutuhkan waktu yang lambat ketika mengenkripsi dan mendekripsi [3]. Maka dari itu, dalam sistem pengamanan ini identitas pelapor akan dijaga kerahasiaannya dan terbukti kebenarannya melalui proses autentikasi, otorisasi, dan enkripsi. Pengamanan *anonym* untuk identitas pelapor pada aplikasi Android ini akan menggunakan algoritma kriptografi ElGamal untuk enkripsi dan dekripsi, *Firebase Auth* untuk autentikasi, serta *Firebase Rules* untuk otorisasi.

## II. KRIPTOGRAFI ELGAMAL

### A. Autentikasi

Proses validasi user pada saat memasuki sistem dinamakan dengan autentikasi. Mengkonfirmasi bahwa seseorang yang hendak memasuki sistem tersebut adalah

<sup>1</sup> Mahasiswa, Program Studi Teknik Elektro Fakultas Teknik Universitas Udayana, Jalan Kampus Bukit Jimbaran 80361 INDONESIA telp: 0361-703315; fax: 0361-703315

<sup>2,3</sup> Staff Pengajar, Program Studi Teknik Elektro Fakultas Teknik Universitas Udayana, Jalan Kampus Bukit Jimbaran 80361 INDONESIA telp: 0361-703315; fax: 0361-703315



orang yang tepat merupakan suatu langkah autentikasi. Proses autentikasi pada sistem komputer terjadi pada saat login. Metode untuk memastikan bahwa dokumen yang diterima memang benar dan tidak berubah adalah dengan autentikasi. Cara untuk memastikan bahwa benar dari orang yg bersangkutan adalah dengan cara mengirimkan suatu kode melalui email dan email tersebut akan dibalas oleh pemiliknya atau menyetujui kembali kode yang dikirim. Metode dari autentikasi dapat digolongkan menjadi empat jenis yaitu: *Something you know*, *Something you have*, *Something you are*, dan *Something you do*.

**B. Kriptografi**

Kriptografi merupakan sebuah fungsi *plaintext* dan kunci kriptografi dapat dirumuskan sebagai berikut:

$$C = F(P, K) \tag{1}$$

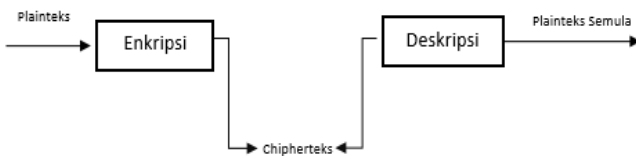
Keterangan:

P = *Plaintext*

C = *Ciphertext*

K = *Cryptographic Key*

Konsep kriptografi seperti pada Gambar 1

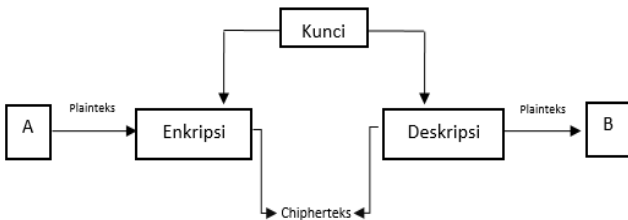


Gambar 1. Gambaran Umum Konsep Kriptografi [7]

Secara umum kriptografi dibagi menjadi dua jenis, yaitu :

**1. Kunci Simetris**

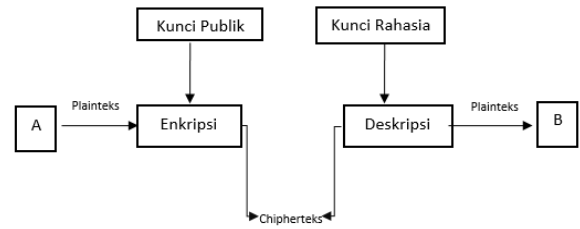
Kunci simetris adalah kriptografi yang menggunakan satu kunci yang sama untuk proses enkripsi dan proses dekripsinya. Contoh algoritma kriptografi simetris seperti DES, AES, RC4, RC6, 3DES. Gambaran umum konsep kriptografi simetris ditunjukkan pada Gambar 2



Gambar 2. Gambaran Umum Kriptografi Simetris [7]

**2. Kunci Asimetris**

Pada kriptografi kunci asimetris menggunakan kunci yang berbeda untuk proses enkripsi dan proses dekripsinya. Dalam proses enkripsi dan dapat diketahui oleh seluruh pengguna adalah kunci publik. Sedangkan untuk kunci rahasia digunakan dalam proses dekripsi dan disimpan atau dijaga keamanannya. Contoh dari algoritma kriptografi asimetris yaitu RSA, DSA, Diffie-Hellman, ElGamal, PKCS. Gambaran umum konsep kriptografi simetris ditunjukkan pada Gambar 3



Gambar 3 Gambaran Umum Kriptografi Asimetris [7]

**C. Algoritma ElGamal**

Algoritma kriptografi ElGamal adalah contoh algoritma dengan kunci asimetris yang didasarkan pada logaritma diskrit. Taher ElGamal yang berasal dari Mesir pada tahun 1984 pertama kali mengembangkan algoritma ELGamal. Penghitungan logaritma diskrit pada bilangan modulo prima yang besar menyebabkan sangat sukar menyelesaikan Algoritma ElGamal. Algoritma ElGamal melakukan proses enkripsi pada blok-blok plaintexts dan akan menghasilkan blok-blok ciphertexts kemudian dilakukan proses dekripsi, yang nanti hasil tersebut akan digabungkan kembali menjadi identitas yang sama seperti plaintexts [4].

ElGamal memiliki kelemahan yaitu prosesnya lebih lama dan memerlukan kapasitas pengiriman lebih besar hal itu dikarenakan ciphertexts identitas yang dihasilkan mempunyai panjang dua kali lipat dari plaintexts identitasnya [1]. Pada plaintexts ElGamal yang sama, jika di enkripsi memberikan ciphertexts yang berbeda. Hal ini dikarenakan pada saat dilakukannya proses enkripsi ada variabel yang ditentukan secara acak. Proses pembentukan kunci, enkripsi dan dekripsi merupakan proses dari algoritma ElGamal. Pada proses algoritma ElGamal terdapat beberapa parameter yang digunakan, yaitu:

- Bilangan prima p merupakan bilangan yang sifatnya tidak rahasia
- g merupakan bilangan acak yang bersifat rahasia
- Bilangan acak x merupakan bilangan yang sifatnya tidak rahasia
- Bilangan y merupakan bilangan yang bersifat tidak rahasia
- m merupakan *Plaintext*
- a dan b merupakan *ciphertext*

Sepasang kunci dibangkitkan pada proses pembentukan kunci dan diambil dari bilangan prima p yang bersifat tidak rahasia serta bilangan acak g dan bilangan acak x dengan syarat  $x < p$  dan  $g < p$ , maka

$$y = g^x \text{ mod } p \tag{2}$$

Kemudian pada proses enkripsi dilakukan dengan cara memilih bilangan acak k dengan syarat  $1 \leq k \leq p - 2$ . Setiap blok *plaintext* dienkripsi dengan persamaan (2) dan (3)

$$a = g^k \text{ mod } p \tag{3}$$

$$b = y^x m \text{ mod } p \tag{4}$$

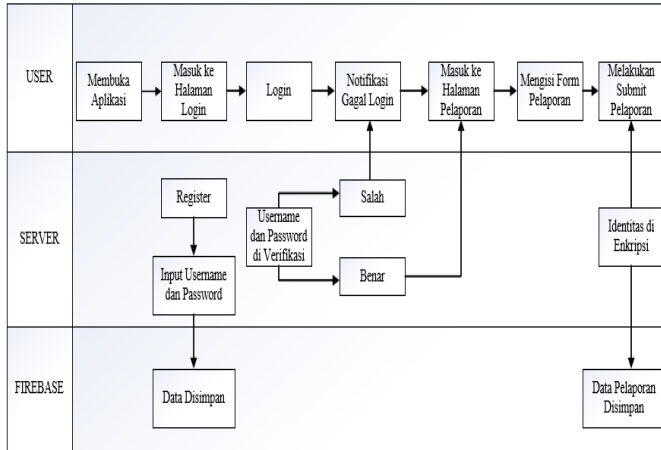
Selanjutnya untuk mendeskripsikan a dan b menjadi *plaintext* pada proses dekripsi menggunakan kunci privat x dan p dengan persamaan:

$$(ax)^{-1} = a^{p-1-x} \text{ mod } p \tag{5}$$

$$m = b \times a^x \text{ mod } p \quad (6)$$

A. HASIL DAN PEMBAHASAN *Gambaran Sistem*

Gambaran dari sistem aplikasi pelaporan tindak kekerasan dalam rumah tangga menggunakan platform android dan database firebase dilihat seperti pada gambar berikut:



Gambar 4. Gambaran Umum Sistem

Gambar 4 merupakan gambaran umum sistem yang terdiri atas tiga bagian yakni *user*, *server*, *database*. Pada bagian *user*, dipaparkan mengenai apa saja aktivitas yang dilakukan oleh *user* dalam aplikasi. Pada bagian *server*, dipaparkan mengenai proses register *user* agar terdaftar dalam aplikasi serta proses otentikasi, otorisasi, dan pengamanan *anonym* yang menjadi sistem keamanan pada aplikasi. Pada bagian *database*, dipaparkan mengenai data-data apa saja yang disimpan baik itu data *user* maupun data pelaporan itu sendiri.

Pada sistem pelaporan tindak kekerasan dalam rumah tangga terdapat dua pengguna yang berbeda yaitu admin dan pengguna biasa. Beberapa kebutuhan fungsional pengguna seperti pada tabel I

TABEL I  
 KEBUTUHAN FUNGSIONAL PENGGUNA

No.	Kebutuhan Fungsional	Keterangan
1.	<i>Email</i>	Pengguna memerlukan <i>email</i> untuk beberapa proses seperti otentikasi, otorisasi dan verifikasi informasi
2.	<i>Password</i>	Pengguna memerlukan <i>password</i> untuk masuk ke sistem melalui proses otentikasi
3.	<i>User UID</i>	Pengguna memerlukan <i>User UID</i> untuk proses otorisasi dan mengakses data pada database

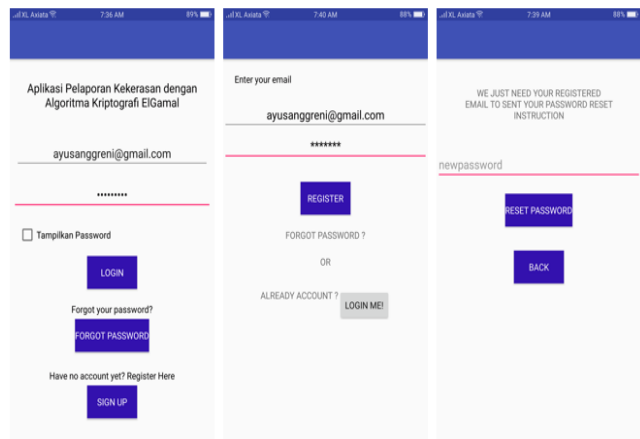
Sedangkan beberapa kebutuhan fungsional dari sistem ditunjukkan pada tabel II

TABEL II  
 KEBUTUHAN FUNGSIONAL SISTEM

No.	Kebutuhan Fungsional	Keterangan
1.	<i>Email</i>	Sistem memerlukan email untuk proses otentikasi, otorisasi dan verifikasi informasi
2.	<i>Password</i>	Sistem memerlukan <i>password</i> untuk masuk ke sistem melalui proses otentikasi
3.	Nomor Telepon	Sistem memerlukan nomor telepon untuk masuk ke dalam sistem melalui proses otentikasi
4.	<i>User UID</i>	Pengguna memerlukan <i>User UID</i> untuk proses otorisasi dan mengakses data pada database
5.	<i>Rules</i>	Sistem memerlukan sebuah <i>rules</i> untuk mendefinisikan hak akses pengguna untuk mengakses database
6.	Data Laporan Kekerasan	Sistem memerlukan data laporan kekerasan untuk disimpan pada database

B. Tampilan Aplikasi

Berikut merupakan tampilan aplikasi tindak kekerasan dalam rumah tangga



Gambar 5. Tampilan halaman Login, Register dan Forgot password

C. Avalanche Effect

Hasil enkripsi dengan menggunakan algoritma kriptografi ElGamal pada aplikasi pelaporan tindak kekerasan dalam rumah tangga ditunjukkan seperti pada gambar 6.







Gambar 6. Tampilan hasil enkripsi pada aplikasi

Algoritma enkripsi ElGamal memiliki masukan *Plain Text* yang akan dikonversikan ke dalam nilai angka desimal dengan menggunakan tabel ASCII sehingga menghasilkan *Cipher Text* berupa angka desimal [6] *Chiper Text* kemudian disimpan dalam *Database* yang selanjutnya akan di konversi menjadi bentuk biner dengan menggunakan konverter biner secara online. Setelah dilakukannya konversi terhadap *Chiper Text* maka dapat diketahui jumlah bit yang berbeda dari *Plain Text* yang telah mengalami sedikit perubahan. Hai ini bertujuan untuk menghitung *avalanche effect*.

Pengujian *Avalanche Effect* dilakukan dengan menggunakan 10 sampel *Plain Text* yang berbeda. Berdasarkan hasil konversi diketahui perbedaan jumlah bit *Cipher Text* seperti pada Tabel III berikut

TABEL III  
PENGUJIAN AVALANCHE EFFECT

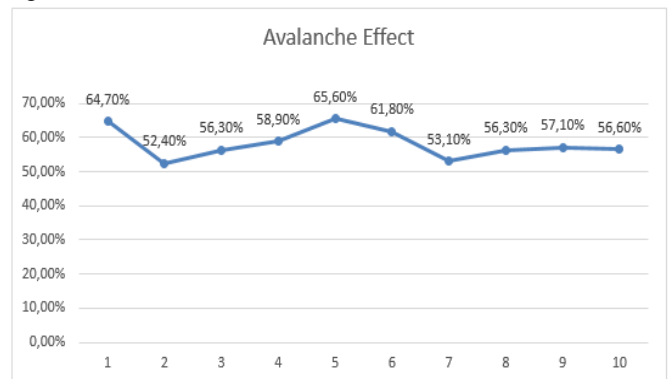
No.	Plain Text	Jumlah Bit Berbeda
1.	Anggreni	368
	Anggremiti	
2.	Cok Ratih	344
	Cok Satih	
3.	Indira	248
	Indisa	
4.	Denpasar	344
	Denpadar	
5.	Pegawai	336
	Pegarai	
6.	Mahasiswa	408
	Mahasiswi	
7.	Renon	200
	Renom	
8.	Panjer	248
	Panjar	
9.	Suariami	352
	Suariami	
No.	Plain Text	Jumlah Bit Berbeda
10.	Perumahan	376
	Perumaham	

Perhitungan *avalanche effect* dapat dilakukan dengan melihat jumlah bit berbeda seperti yang ditunjukkan pada Tabel III. Sehingga nilai hasil perhitungan *avalanche effect* seperti pada tabel IV

TABEL IV  
HASIL PERHITUNGAN AVALANCHE EFFECT

No.	Plain Text	Avalanche Effect
1.	Anggreni	64,7 %
	Anggremiti	
2.	Cok Ratih	52,4 %
	Cok Satih	
3.	Indira	56,3 %
	Indisa	
4.	Denpasar	58,9 %
	Denpadar	
5.	Pegawai	65,6 %
	Pegarai	
6.	Mahasiswa	61,8 %
	Mahasiswi	
7.	Renon	53,1 %
	Renom	
8.	Panjer	56,3 %
	Panjar	
9.	Suariami	57,1 %
	Suariami	
10.	Perumahan	56,6 %
	Perumaham	

Berdasarkan hasil perhitungan *Avalanche Effect* dari 10 sampel yang digunakan dapat dilihat seperti grafik pada gambar 7



Gambar 7 Grafik Avalanche Effect

Grafik pada gambar 7 menunjukkan hasil perhitungan *Avalanche Effect* berkisar antara 50-60%. Dengan menggunakan 10 sampel *cipher text* rata-rata *Avalanche Effect* keseluruhan adalah 58,2%. Hal ini menunjukkan bahwa proses pengamanan yang dilakukan telah dikategorikan baik karena telah memenuhi syarat dari *Avalanche Effect* yaitu keluaran perhitungan atas perubahan bit menghasilkan 40-60 % dari keseluruhan bit *Cipher Text*.

### III. KESIMPULAN

Berdasarkan hasil penelitian dapat dilihat bahwa algoritma enkripsi ElGamal memiliki masukan *Plain Text* yang akan dikonversikan ke dalam nilai angka desimal dengan menggunakan tabel ASCII sehingga menghasilkan *Cipher Text* berupa angka desimal.

Tingkat keamanan aplikasi pelaporan tindak kekerasan dalam rumah tangga ini dinyatakan aman dari serangan kriptanalisis yang diukur dari pengujian Avalanche Effect dengan menggunakan 10 cipher text yang berbeda didapatkan hasil rata-rata avalanche effect sebesar 58,2 % dimana hasil tersebut dikategorikan baik mengingat syarat dari Avalanche Effect yaitu keluaran perhitungan atas perubahan bit menghasilkan 40-60 % dari keseluruhan bit Cipher Text.

#### REFERENSI

- [1] Al-Anshori, Faqihuddin., Aribowo, Eko. 2014. *Impelementasi Algoritma Kriptografi Kunci Publik ElGamal Untuk Proses Enkripsi dan Dekripsi Guna Pengamanan File Data. Jurnal Sarjana Teknik Informatika, Vol.2 No.2*
- [2] Himawan, Cindy., Wibowo, Toni., Sulisty, Budi. 2016. *Studi Perbandingan Algoritma RSA dan Algoritma El-Gamal.* Presiden University.
- [3] Sharma, Ankush., Attri, Jyoti., Devi, Aarti., Sharma, Pratibha. 2014. *Implementation & Analysis of RSA and ElGamal Algorithm.* Asian J. of Adv. BasicSci : 2(3). 125-129
- [4] Mulya, Megah., 2013. *Perbandingan Kecepatan Algoritma Kriptografi Asimetri. Journal of Research in Computer Science and Applications, Vol.1 No.2*
- [5] Karima, Aisyatul., Handoko, L. Budi., Saputro, Ari. 2017. *Pemfaktoran Bilangan Prima pada Algoritma ElGamal untuk Keamanan Dokumen PDF.* JNTETI, Vol.6, No.3
- [6] Triase. 2015. *Kriptografi ElGamal Menggunakan Metode Mersenne. Jurnal Ilmiah "Integritas". Vol.1 No.4*
- [7] Kabetta, Herman. 2017. *Analisis Kompleksitas Waktu Algoritma Kriptografi ElGamal dan Data Encryption Standard. Jurnal Teknikom. Vol.1 No.1 ISSN: 2598-294X*
- [8] Parmadi, B. (2017). *Implementasi Algoritma Kriptografi Elgamal pada Data Text, Journal of Information and Technology, Vol.05 No 01.*
- [9] Vishwakarma, Manila., Jain Sourabh. (2018). *An Efficient Cryptosystem to Perform Encryption and Decryption of Data.*
- [10] Djellalbia, Amina., Badache, Nadjib., Benmeziane, Souad., Bensimessaoud, Sihem. 2016. *Anonymous Authentication Scheme in e-Health Cloud Environment. 11<sup>th</sup> International Conference for Internet Technology and Secured Transactions (ICITST). 47-52*
- [11] Nivedita Bisht dan Sapna Singh.. "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms". *International Journal of Innovative Research in Science Engineering and Technology Vol. 4 Issue 3. 2015.*



{ halaman ini sengaja di kosongkan }