# IMPLEMENTASI KRIPTOGRAFI KEAMANAN DATA RESI PADA PT JNE PERBAUNGAN MENGGUNAKAN METODE MERKLE HELLMAN

**Ade Citra Ningati*, Widiarti Rista Maya, ST., M.Kom**, Usti Fatimah Sari Sitorus Pane, S.Kom., M.Kom****

*Program Studi Sistem Informasi, STMIK Triguna Dharma

**Program Studi Sistem Informasi, STMIK Triguna Dharma

**Article Info**

***Article history:***
Recaived
Revised
Accepted

***Keyword:***
***Pengamanan, Kriptografi, Merkle Hellman.***

**ABSTRACT**

*Pada PT. JNE data resi dapat diamankan karena tidak hanya keamanan data resi sehingga mengakibatkan costumer untuk mengecek data resi selalu terhambat. Pada pemasalahan tersebut di butuhkan ilmu kriptografi dalam mengamankan data resi metode Merkle Hellman.*

*Untuk mempermudah dalam mengamankan data dapat menggunakan Kriptografi. Banyak metode yang dapat digunakan, salah satunya dengan menggunakan metode Merkle Hellman dalam pengambilan keamanan yang tepat.*

*Penerapan metode ini yang dimasukkan kedalam coding program dengan implementasi Kriptografi keamanan Data pengujian sistem berdasarkan data yang telah diinputkan dapat membantu mengamankan data resi pada PT. JNE Perbaungan*



First Author
Nama : Ade Citra Ningati
Program Studi : Sistem Informasi
STMIK Triguna Dharma
E-Mail : citraadeningati@gmail.com

## 1. PENDAHULUAN

Keamanan data resi pengiriman barang *online shop* harus memiliki suatu proses aspek yang wajib di lindungi dan di jaga keaslian datanya. Bagaimana pun data resi pegiriman barang tersebut harus di amankan, karena takut ada pihak yang tidak bertanggung jawab mengubah atau memanipulasi data resi tersebut. Maka dari itu sangat penting di amankan dan dapat di minimalisir dengan ilmu kriptografi. Pengamanan data adalah salah satu pembahasan yang begitu penting dari . teknologi informasi pada saat ini.

Kriptografi adalah salah satu alternatif ilmu matematika yang mentransformasikan data jelas *plaintext* kedalam bentuk data sandi atau *ciphertext*. Proses enkripsi adalah pengubahan *plaintext* menjadi *chipertext* (dengan menggunakan kunci yang sudah ditetapkan atau kunci tertentu), informasi atau data tersebut susah untuk di pahami. Proses dekripsi di sebut pengubahan *chipertext* menjadi *plaintext*, proses ini di gunakan untuk mengubah data yang sudah di enkripsi menjadi data seperti semula.

## 2. METODE PENELITIAN

### 2.1 Kriptografi

Kriptografi pada awalnya diartikan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Kriptografi adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. *Plaintext* adalah data asli, data yang masih bisa di baca dan di mengerti.

Kriptografi berasal dari Bahasa Yunani, *cryptho* dan *graphia*. *Cryptho* berarti *secret* (rahasia) dan *Graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi sebuah informasi dapat di acak atau di sandikan menjadi informasi yang sulit atau bahkan tidak di pahami melalui sebuah proses yang di namakan dengan enkripsi (Murdani, 2017).

Kriptografi di perlukan karena pada dasar nya informasi sangat peting bagi segala aspek, tuntutan kemanan informasi berubah dari waktu ke waktu. Perubahan tuntutan ini terjadi karena transformasi atau penggunaan perlengkapan kebutuhan utama untuk pertukaran informasi, dari mulai cara tradisional (fisik) yang membutuhkan mekansime pengarsipan atau administrasi secara fisik dan membutuhkan ruang yang lebih besar, mengguna kan otomatisasi komputer personal, sampai transfer informasi melalui penggunaan jaringan komputer, baik *intranet* maupun *internet* yang sekarang menjadi tren dan kebutuhan.

### 2.2 Merkle Hellman

Merkle hellman merupakan metode dalam kriptografi yang menggunakan algoritma asimetris dan memiliki 2 kunci utama, yakni kunci publik dan kunci private di banding kan dengan atribut lain (Agarwal,2011 : 270).

Dengan Merkle Hellman di lakukan dengan proses enkripsi dan dekripsi menggunakan kunci ganda untuk pengamanan data-data rahasia yang sangat penting.Merkle hellman memiliki algoritma yang berbeda pada pada proses enkripsi dan dekripsi.



Langkah-langkah pengamanan *Merkle Hellman* adalah sebagai berikut :

1. Proses Enkripsi

   Langkah-langkah proses enkripsi sebagai berikut:

   a. Nilai w, q, dan r adalah variable untuk *private key*. Angka-angka bilangan bulat yang di susun dengan algoritma *superincreasing* linear. w terdiri dari beberapa angka tergantung dari jumlah digit biner yang di gunakan. q adalah nilai (angka bebas yang harus lebih besar dari jumlah keseluruhan nilai w. Sedangkan r adalah nilai (angka) bebas yang dapat di ambil mulai dari angka 1 sampai dengan nilai q..

   b. Membuat Public Key

      *Public key* di gunakan untuk menghitung chipper data.

      *Public key* memiliki karakter yang sama dengan *private key* w.

      Jika *private key* di lambangkan dengan w, maka *public key* dapat di lambangkan dengan β karna itu *public key* memiliki deretan angka sebagai kunci untuk mencari chipper.

   c. Merubah Plainteks ke Binner 8 Digit

      Pada proses ini data perlu dirubah menjadi bentuk binner karena perhitungan *Merkle Hellman* menggunakan teknik binary sebagai proses enkripsi dan dekripsinya. Untuk mengubah data ke binary 8 digit, maka sebelumnya data dirubah ke kode ASCII. Langkah selanjutnya adalah mengubah kode ASCII tersebut menjadi kode binary 8 digit

   d. Menjumlahkan (Perkalian Binner dengan *Public Key*)

      Untuk proses perhitungan data *chippertext*, terlebih dahulu harus melakukan pembagian *plaintext* ke dalam blok-blok berdasarkan jumlah elemen T. Diketahui jumlah elemen T sebanyak 8 elemen. Selanjutnya, setiap blok akan dikaitkan dengan setiap elemen T, sehingga diperoleh *chippertext*.

2. Proses Dekripsi
   Langkah-langkah dalam proses dekripsi dengan menggunakan metode *Merkle Hellman* adalah sebagai berikut :
   a. Data Chippertext (O)
      Dalam melakukan proses dekripsi, terlebih dahulu harus ada data yang lengkap.
   b. Modular *Invers*
      Proses untuk mencari nilai modulo invers dari ($r^{-1}$) dengan menggunakan metode extended eucledian. Dalam proses dekripsi ini akan menggunakan nilai $r^{-1}$. Nilai M diperoleh dari hasil perhitungan menggunakan metode extended eucledian. M = (r*M mod p= 1) . . . . .[2.6]

   c. *Chipper* Data Mod A
      Proses berikutnya adalah proses mod, yaitu untuk data chippertext dengan nilai invers yang diperoleh.

   d. Mengurangkan Data dengan Nilai W
      Proses Pengurangan data (K) dengan nilai-nilai pada elemen S. Pengurangan terus dilakukan dari elemen yang paling besar hingga yang paling kecil. Hasil akhir dari pengurangan haruslah bernilai 0. Hasil akhir dimana pengurangan tidak nol, maka proses dekripsi dinyatakan gagal. Penyebab kegagalan dapat terjadi apabila kunci S tidak dibuat dengan metode siperincreasing linier

## 3. ANALISA DAN HASIL

### 3.1 Analisis

Masalah data Resi Pengiriman barang *online shop* adalah salah satu aspek data umum yang penting pada kantor Jne Perbaungan agar data aman dan tidak dapat di manipulasi oleh orang-orang yang tidak bertanggung jawab. Kadang masalah keamanan ini sering kurang dapat perhatian oleh pihak pekerja.

Permasalahan yang terdapat pada data resi di Jne Perbaungan adalah data resi belum dihosting dan masih hanya menggunakan *internet* biasa atau pun di sebut paket kuota yang terbatas yang dapat diakses didalam jaringan yang sama.



### 3.2 Hasil

Adapun langkah-langkah proses enkripsi dari suatu data dengan menggunakan metode *Merkle Hellman* adalah sebagai berikut :

1. Membuat *Private Key* (A, D dan E)

Nilai A, M, dan Y adalah variable untuk *private key*.Angka-angka bilangan bulat yang disusun dengan algoritma superincreasing linear.A terdiri dari beberapa angka tergantung dari jumlah digit binner yang digunakan.M adalah nilai (angka) bebas yang harus lebih besar dari jumlah keseluruhan nilai Y dengan maksimal nilai 999.Sedangkan Y adalah nilai (angka) bebas yang dapat diambil mulai dari angka 1 sampai dengan nilai A.

Tabel 1 *Private Key*

| | |
|---|---|
| **A** | {2,6,8,18,30,112,220,400}= ∑A = 796 |
| **D** | 989 |
| **E** | 578 |

2. Membuat *Public Key*

*Public key* digunakan untuk menghitung hasil chipper data.*Public key* memiliki karakter yang sama dengan *private key* A. Jika *private key* dilambangkan dengan A, maka *public key* dapat dilambangkan dengan P. Karena itu *public key* memiliki deretan angka sebagai kunci untuk mencari chipper. Perhitungan *public key* seperti tabel di bawah ini:

Tabel 2 *Public Key*

| **A** | **P = ( E * Wi ) mod D** | **P** |
|---|---|---|
| 2 | 578 * 2 mod 989 | 167 |
| 3 | 578 * 3 mod 989 | 501 |

| | | |
|---|---|---|
| 6 | 578 * 6 mod 989 | 668 |
| 18 | 578 * 18 mod 989 | 514 |
| 30 | 578 * 30 mod 989 | 527 |
| 112 | 578 * 112 mod 989 | 451 |
| 220 | 578 * 220 mod 989 | 568 |
| 400 | 578 * 400 mod 989 | 763 |

Maka hasil proses Public Key adalah : P = {167,501,668,514,360,65,438,763}

3. Merubah Plainteks ke Binner 8 Bit

Pada proses ini data perlu dirubah menjadi bentuk binner karena perhitungan *Merkle Hellman* menggunakan teknik *binary* sebagai proses enkripsi dan dekripsinya. Untuk mengubah data ke binary 8 bit, maka sebelumnya data dirubah ke kode ASCII.

Langkah selanjutnya adalah mengubah kode ASCII tersebut menjadi kode binary 8 bit, yaitu :

Tabel 3 Data *Binary*

| Plaintext | ASCII | Binnary |
|---|---|---|
| 0 | 48 | 00110000 |
| 6 | 54 | 00110110 |
| 1 | 49 | 00110001 |
| 8 | 56 | 00111000 |
| 1 | 49 | 00110001 |
| 0 | 48 | 00110000 |
| 0 | 48 | 00110000 |
| 1 | 49 | 00110001 |
| 3 | 51 | 00110011 |
| 3 | 51 | 00110011 |
| 6 | 54 | 00110110 |
| 7 | 55 | 00110111 |

4. Menjumlahkan (Perkalian Binner dengan *Public Key*)

Untuk proses perhitungan data *ciphertext*, terlebih dahulu harus melakukan pembagian *plaintext* ke dalam blok-blok berdasarkan jumlah elemen P. Diketahui jumlah elemen P sebanyak

8 elemen.

Selanjutnya, setiap blok akan dikaitkan dengan setiap elemen P, sehingga diperoleh *ciphertext* sebagai berikut:

| Binary (z) | ∑z * P | Chippertext |
|---|---|---|
| 00110000 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(0*451)+(0*568)+(0*763) | 1182 |
| 00110110 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(1*451)+(1*568)+(0*763) | 2201 |
| 00110001 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(0*451)+(0*568)+(1*763) | 1945 |
| 00111000 | (0*167)+(0*501)+(1*668)+(1*514)+(1*527)+(0*451)+(0*568)+(0*763) | 1709 |
| 00110001 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(0*451)+(0*568)+(1*763) | 1945 |
| 00110000 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(0*451)+(0*568)+(0*763) | 1182 |
| 00110000 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(0*451)+(0*568)+(0*763) | 1182 |
| 00110001 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(0*451)+(0*568)+(1*763) | 1945 |
| 00110011 | (0*167)+(0*501)+(1*668)+(1*504)+(0*527)+(0*451)+(1*568)+(1*763) | 2503 |
| 00110011 | (0*167)+(0*501)+(1*668)+(1*504)+(0*527)+(0*451)+(1*568)+(1*763) | 2503 |
| 00110110 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(1*451)+(1*568)+(0*763) | 2201 |
| 00110111 | (0*167)+(0*501)+(1*668)+(1*514)+(0*527)+(1*451)+(1*568)+(1*763) | 2964 |

Tabel 4 Perhitungan Data *Chippertext*

Proses diatas menunjukan bahwa proses enkripsi data sudah selesai dilakukan. Hal terakhir yang dilakukan adalah menyajikan data *chippertext* dengan menyimpan kembali kedalam bentuk dokumen.

Hasil proses enkripsi dari pesan “061890012267” adalah

C = {1182,2201,1945,1709,2472,1182,1182,1945,1750,1750,2201,2964}

Tabel 5 Modular *Invers*

| M | ( E * M ) mod D | |
|---|---|---|
| 1 | 578 * 1 mod 989 | 578 |
| 2 | 578 * 2 mod 989 | 167 |
| 3 | 578 * 3 mod 989 | 745 |
| … | … | … |
| 77 | 578 * 77 mod 989 | 1 |

1. *Chipper* Data Mod D

Proses berikutnya adalah proses mod, yaitu untuk data *ciphertext* dengan nilai *invers* yang diperoleh sebelumnya. Proses *ciphertext* data mod adapat dilihat pada table di bawah ini :

| Chipper ( C ) | M | K = (C * M) mod D | |
|---|---|---|---|
| 1182 | 77 | 1182*77 mod 989 | 26 |
| 2201 | 77 | 2201*77 mod 989 | 358 |
| 1945 | 77 | 1945*77 mod 989 | 426 |
| 1709 | 77 | 1709*77 mod 989 | 56 |
| 2472 | 77 | 247*77 mod 989 | 456 |
| 1182 | 77 | 1182*77 mod 989 | 26 |
| 1182 | 77 | 1182*77 mod 989 | 26 |
| 1945 | 77 | 1945*77 mod 989 | 426 |
| 1750 | 77 | 1750*77 mod 989 | 246 |
| 1750 | 77 | 1750*77 mod 989 | 246 |
| 2201 | 77 | 2201*77 mod 989 | 358 |
| 2964 | 77 | 2964*77 mod 989 | 758 |

Tabel 6 *Chipper* Data Mod M



2. Mengurangkan Data Dengan Nilai A
   Proses pengurangan data (K) dengan nilai-nilai pada elemen A. Pengurangan terus dilakukan dari elemen yang paling besar hingga yang paling kecil. Hasil akhir dari pengurangan haruslah bernilai 0. Hasil akhir dimana pengurangan tidak nol, maka proses dekripsi dinyatakan gagal. Penyebab kegagalan dapat terjadi apabila kunci A tidak dibuat dengan metode *superincreasinglinier*. A = {2,6,8,18,30,112,220,400},
   K = {26,358,426,56,456,26,26,426,246,246,358,758 }.

| 2 | 6 | 8 | 18 | 30 | 80 | 100 | 400 | S |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | 26-400 | K |
| | | | | | | 26-220 | | |
| | | | | | 26-112 | | | |
| | | | | 26-30 | | | | |
| | | | 26-18 | | | | | |
| | | 8-8 | | | | | | |
| | 0-6 | | | | | | | |
| 0-2 | | | | | | | | |
| | | | | | | | | |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | |

Tabel 7 Proses Pengurangan Data dengan Nilai A

Proses perhitungan pada tabel di atas mulai dari kanan ke kiri, kolom yang diberi tanda false berarti pada elemen A kolom tersebut data tidak dapat dikurangi dan akan bernilai false atau 0. Sedangkan kolom yang berisi data true, berarti data dapat dikurangkan dan bernilai true atau 1. Apabila hasil data tersebut diambil keseluruhan maka akan menghasilkan nilai "00110000" yang apabila dikembangkan ke kode decimal menjadi "48" Dan ke char menjadi "0".

**4. Pengujian**

i. F *orm Login*

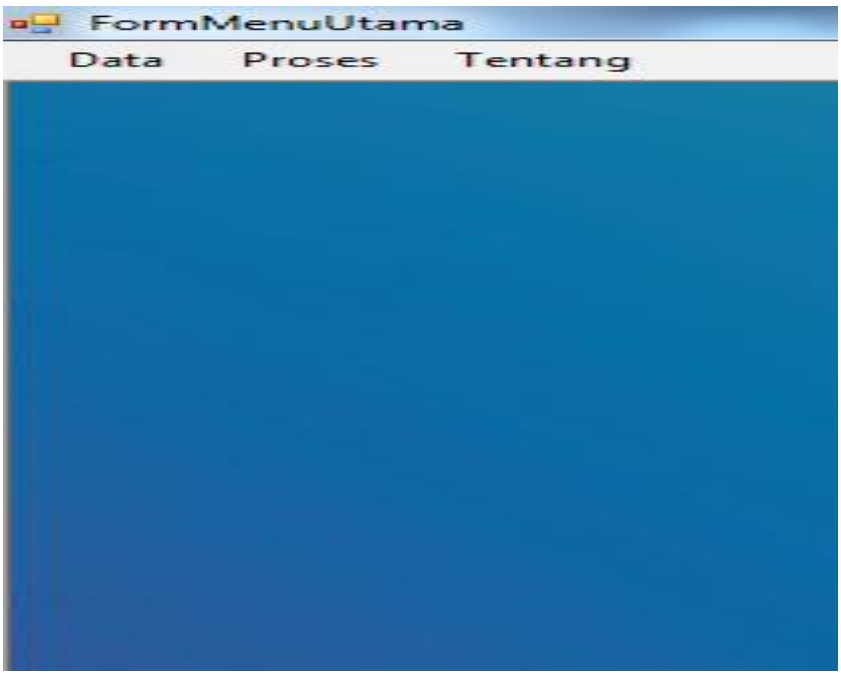
Form login merupakan form yang akan muncul pertama kali pada saat dijalankan. Seperti pada sistem umumnya, sebuah aplikasi dengan adanya sistem *login* akan memberikan kemudahan pengguna untuk keamanan sistem yang telah dirancang. Berikut merupakan tampilan sistem *login* pada aplikasi ini :


Gambar 1 *Form* Login

e. Tampilan Form Menu Utama

Halaman utama merupakan halaman pembuka aplikasi kriptografi *Merkle Hellman* untuk mengamankan data resi keamanan data , setelah *user* melakukan proses *login* terlebih dahulu. Adapun tampilan dari halaman menu utama adalah sebagai berikut :

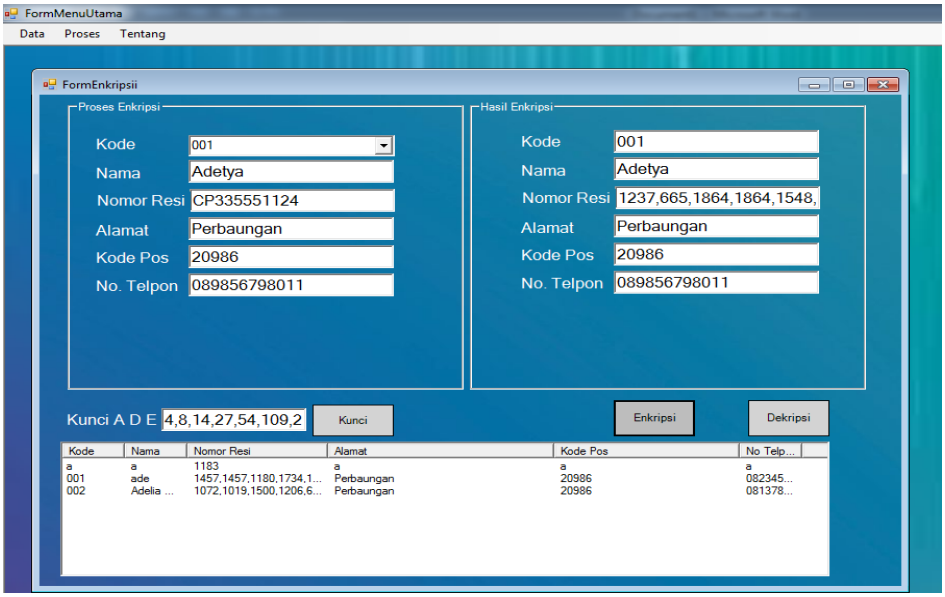





Gambar 2 Tampilan Form Menu Utama

*f. Form* Enkripsi

Setelah melakukan proses implementasi, proses selanjutnya adalah uji coba dengan mengetahui bahwa hasil perancangan sesuai dengan hasil yang ditampilkan pada aplikasi. Setelah melakukan pengujian, untuk hasil perhitungan dan keluaran berupa hasil enkripsi berisi *ciphertext*, berikut hasil pengujian aplikasi yang telah dibangun :

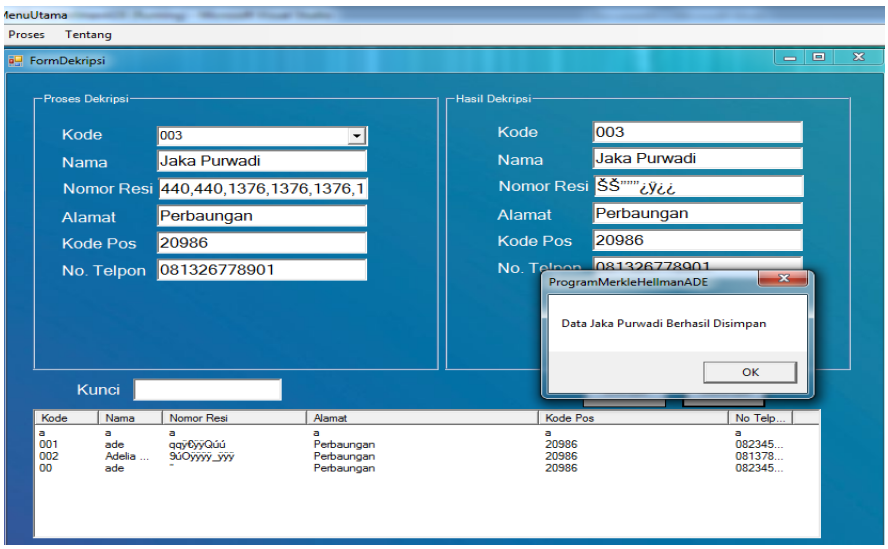



Gambar 3 Tampilan Data Resi CP35551124 Berisi Pesan Hasil Enkripsi



**g.** *Form* Dekripsi

*Form* dekripsi dibawah ini digunakan untuk melakukan proses pengembalian data terhadap data yang telah dilakukan proses enkripsi.




Gambar 5 Tampilan Pengembalian Data Resi 001118B88 melalui Proses Dekripsi

h. Kesimpulan

Kesimpulan yang terdapat dari proses kriptografi untuk pengamanan data resi pada PT JNE Perbaungan menggunakan *Markle Helman*

1. Dapat mengamankan data berdasarkan resi tersebut membuat sebuah program kriptografi untuk mengamankan data resi pada PT. JNE Perbaungan.
2. Dalam merancang dan membangun aplikasi kriptografi kemanan data resi pada PT.JNE menggunakan metode *Markle Hellman* dilakukan dengan cara menerapkan konsep-konsep flowchart,UML (Unified Modeling Language) dan Desktop Programming didalamnya yang dimana flowchart dan UML tersebut merupakan gambaran arsitektur dari program yang dibuat.
3. Dapat mengamakan data agar dapat digunakan dalam mengamankan data tersebut.

REFERENSI

Andoyo, A., & Rianto, R. (n.d.). PROGRAM APLIKASI NILAI SISWA PADA SMK MUHAMMADIYAH PRINGSEWU SEBAGAI PENUNJANG PENGAMBILAN KEPUTUSAN SISWA BERPRESTASI MENGGUNAKAN VISUAL BASIC 6 . 0.

Bank, P., & Bhakti, Y. (2014). test 1, *8*(2), 61–69.

Basic, V., Sumsel, B., & Cabang, B. (2017). SISTEM INFORMASI DOKUMENTASI DAN KEARSIPAN BERBASIS CLIENT-SERVER PADA BANK SUMSEL BABEL CABANG SEKAYU Ekkal Prasetyo Program Studi Teknik Informatika Politeknik Sekayu Email excal.polsky@gmail.com, *VII*(2), 1–10.

Destiningrum, M., & Adrian, Q. J. (2017). SISTEM INFORMASI PENJADWALAN DOKTER BERBASSIS WEB DENGAN MENGGUNAKAN FRAMEWORK CODEIGNITER ( STUDI KASUS : RUMAH SAKIT YUKUM MEDICAL CENTRE ), *11*(2), 30–37.

Fadlan, M., Informasi, S., Tarakan, K., Informatika, T., & Tarakan, K. (2017). Rekayasa aplikasi kriptografi dengan penerapan kombinasi algoritma knapsack merkle hellman dan affine cipher, *4*(4), 268–274. https://doi.org/10.25126/jtiik.201744468

Harahap, M. K. (n.d.). ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD, (190), 61–64.

Hondro, R. K. (2017). ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA TRIANGLE CHAIN CIPHER ( TCC ) UNTUK ENKRIPSI RECORD TABEL DATABASE SYSTEM ANALYSIS AND DESIGN USING TRIANGLE CHAIN CIPHER, (May).

Mulawarman, J. I., Pabokory, F. N., Astuti, I. F., Kridalaksana, A. H., Studi, P., Komputer, I., … Dokumen, I. F. (2015). IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS , ISI FILE DOKUMEN , DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION, *10*(1).

Nasrun, M., Teknik, F., Telkom, U., Teknik, F., Telkom, U., Teknik, F., & Telkom, U. (2015). ANALISIS PERBANDINGAN ANTARA ALGORITMA KRIPTOGRAFI SERPENT DAN AES PADA IMPLEMENTASI ENKRIPSI SMS DI PERANGKAT ANDROID ANALISYS OF COMPARATION BETWEEN CRYPTOGRAPHIC ALGORITHM SERPENT AND AES IN SMS ENCRYPTION ON ANDROID DEVICE IMPLEMENTATION, *2*(2), 3511–3517.

[10] Rifai, A., & Larsson, A. (2016). Aplikasi Kriptografi Database MySQLMenggunakan Metode Markel Helman, *1*(2), 40–46

Sari, A. M., & Yulianti, L. (2015). APLIKASI PENDATAAN PASIEN RUJUK BALIK PESERTA BADAN PENYELENGGARA JAMINAN SOSIAL ( BPJS ) BENGKULU, *11*(2).

Tasikmalaya, D. I., Informatika, T., & Dci, S. (2018). Aplikasi pengolahan data stok mobil pada dealer xyz di tasikmalaya 1, *1*(1).



BIOGRAFI PENULIS

| | |
|---|---|
|  | **Ade Citra Ningati,** Kelahiran Perbaungan, 03 Desember 1996 anak ke empat dari Alm. Bapak Sudarno dan Almh. Sutriatik. |
| | |
|  | **Widiarti Rista Maya, ST., M.Kom** Beliau merupakan dosen tetap STMIK Triguna Dharma, Beliau aktif sebagai dosen khususnya pada bidang Sistem Informasi. |
| | |
| | **Usti Fatimah Sari Sitorus Pane, S.Kom., M.Kom** merupakan dosen tetap STMIK Triguna Dharma, Beliau aktif sebagai dosen khususnya pada bidang Sistem Informasi. |