

---

## Security Serial Number Product Pada PT. Dayamega Pratama Medan Dengan Menggunakan Metode Merkle Hellman

Agnes Synthya Rg\*, Azanuddin\*\*, Jufri Halim\*\*

\* Program Studi Sistem Informasi, STMIK Triguna Dharma

\*\* Program Studi Sistem Informasi, STMIK Triguna Dharma

---

### Article Info

#### Article history:

Received April 12<sup>th</sup>, 2018

Revised April 20<sup>th</sup>, 2018

Accepted April 26<sup>th</sup>, 2018

---

#### Keyword:

*Serial Number, Security, Merkle  
Hellman, PT. Dayamega Pratama*

---

### ABSTRACT

Serial Number atau nomor seri yang tertera pada barang, memiliki arti penting yang signifikan. Arti penting itu misalnya dalam mengatasi klaim garansi, pengecekan stok barang masuk/keluar, pencegahan duplikan/pembajakan barang bahkan pada saat ini dapat digunakan sebagai acuan untuk perhitungan incentive penjualan barang komputer laptop. PT. Dayamega Pratama Medan adalah salah satu perusahaan distribusi laptop yang menggunakan data serial number produk sebagai acuan perhitungan incentive salesman atau retailer. Namun, PT. Dayamega Pratama tidak memiliki sistem keamanan data serial number sehingga data hanya disimpan dalam sebuah folder komputer dengan demikian memungkinkan orang yang berkepentingan terhadap data serial number dapat dengan mudah mengakses komputer tersebut dan mencuri datanya. Dari permasalahan yang terjadi, dengan membangun sebuah sistem security komputer akan dapat membantu penyelesaian permasalahan yang terjadi pada PT. Dayamega Pratama dengan menggunakan metode Merkle Hellman. Hasil dari penelitian ini adalah aplikasi security atau keamanan komputer keputusan dengan metode Merkle Hellman berbasis dekstop yang mampu menyelesaikan permasalahan yang ada pada PT. Dayamega Pratama Medan .

Copyright © 2018 STMIK Triguna Dharma.

All rights reserved.

---

### First Author

Nama : Agnes Synthya Rg  
Kampus : STMIK Triguna Dharma  
Program Studi : Sistem Informasi  
E-Mail : agnessynthya8@gmail.com

---

## 1. PENDAHULUAN

*Serial Number* atau nomor seri adalah suatu

kumpulan karakter unik yang terdiri dari kombinasi antara alfabet dan numerik (alfanumerik) yang menjadi nama atau penanda barang produksi. Biasanya *Serial Number* dibuat selalu berbeda-beda meskipun jenis barangnya sama. Serial number juga umumnya digunakan sebagai kunci *software* berbayar dan bisa didapatkan pengguna setelah membeli *software*.

*Serial Number* atau nomor seri yang tertera pada barang, memiliki arti penting yang signifikan. Arti penting itu misalnya dalam mengatasi klaim garansi, pengecekan stok barang masuk/keluar, pencegahan duplikan/pembajakan barang bahkan pada saat ini dapat digunakan sebagai acuan untuk perhitungan *incentive* penjualan barang komputer laptop.[1]

Berdasarkan pengamatan yang dilakukan di PT.Dayamega Pratama, salah satu perusahaan yang bergerak di bidang pemasok (*supplier*) produk komputer laptop dengan merk Lenovo di Medan. Perusahaan ini menggunakan sebuah aplikasi yaitu Lenovo Indonesia *Retail Automation* (Lenovo IRA) yang berbasis *mobile* dan *web* sebagai aplikasi *monitoring* yang bertujuan untuk memudahkan *salesman* dan *retailer* (pengecer) produk Lenovo dalam melaporkan *incentive* penjualan produk-produk Lenovo dengan cara melakukan *input* per-SN (*Serial Number*) pada aplikasi. Adapun PT. Dayamega Pratama memiliki kelemahan dalam mengamankan data *Serial Number* atau nomor seri, dimana data hanya diarsipkan oleh admin di dalam sebuah folder komputer tanpa memiliki keamanan lebih untuk mengamankan setiap data dan memungkinkan setiap orang di dalam perusahaan bisa saja mengakses data tersebut. Dengan penyimpanan data seperti itu memungkinkan untuk orang lain dapat mencuri atau memanipulasi data. Dengan perkembangan teknologi komputer, kerahasiaan data dapat diminimalisir dengan ilmu kriptografi.

Kriptografi adalah ilmu matematika yang memiliki banyak fungsi dalam mengamankan data. Kriptografi terdiri dari dua proses utama yakni proses enkripsi dan dekripsi. Proses enkripsi adalah mengubah *Plaintext* menjadi *Ciphertext* (dengan memakai kunci tertentu) sehingga informasi pada data tersebut susah untuk dimengerti[2]. Salah satu metode kriptografi yang digunakan dalam pengamanan data adalah metode *Merkle Hellman*

Sistem kriptografi *Merkle Hellman* ditemukan oleh Merkle dan Hellman pada tahun 1980. Algoritma *Merkle Hellman* memakai kunci asimetris dalam proses operasi enkripsi dan dekripsinya[3]. Metode ini menyandikan data dengan cara mengubah hitungan-hitungan data sehingga dapat menghasilkan data-data baru yang tidak dapat dibaca ataupun dipahami oleh pihak-pihak yang tidak berkepentingan. Sehingga dapat membantu dalam menyelesaikan masalah sesuai dengan yang diharapkan.

Berdasarkan permasalahan yang disebutkan, maka diangkatlah sebuah judul "**Security Serial Number Product Pada PT.Dayamega Pratama Medan Dengan Metode Merkle Hellman**"

## 2. KAJIAN PUSTAKA

### 2.1 Security

Security termasuk ke dalam bahasa rumpun Jermanik Barat yang awalnya dituturkan di Negara Inggris pada Abad Pertengahan Awal dan saat ini merupakan bahasa yang paling umum digunakan di seluruh dunia. Security dalam bahasa Indonesianya memiliki arti keamanan. Arti lainnya dari kata security adalah perlindungan.

#### 2.1.1 Keamanan Data

Secara definisi keamanan data adalah usaha untuk melindungi dan menjamin tiga aspek terpenting dalam dunia siber yaitu : kerahasiaan data, keutuhan data, ketersediaan data. [4]

Kerahasiaan data menjamin pengguna siber terlindungi privasinya baik itu privasi yang berada pada komputer pribadi, piranti genggam maupun terlindungi data privasinya ketika melakukan berbagai aktifitas jelajah internet. Keutuhan data menjamin pengguna siber mendapatkan data yang utuh dan benar tanpa dimodifikasi dan dirubah pihak lain ditengah-tengah jalan. Ketersediaan data menjamin pengguna siber mendapatkan data pada saat yang diinginkannya tanpa ditutupi dan tanpa dicegah oleh pihak lain.

#### 2.1.2 Kriptografi

Kriptografi merupakan seni dan ilmu untuk memproteksi kerahasiaan data dengan mengubahnya atau menyandikannya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali.[5] Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Jadi pengertian kriptografi modern adalah tidak saja berurusan dengan penyembunyian pesan namun lebih lagi kepada sekumpulan teknik yang menyediakan keamanan informasi.

## 3. METODE PENELITIAN

### 3.1 Metodologi Penelitian

Dalam suatu penelitian harus memiliki pedoman selama proses penelitian, agar hasil penelitian sesuai dengan tujuan yang ditetapkan. Penelitian merupakan pencarian yang memiliki tujuan untuk menemukan pengetahuan atau harapan baru. Sehingga melalui pengetahuan baru tersebut dapat bermanfaat dalam mengembangkan suatu hal di masa depannya.

Metode penelitian adalah metode atau langkah-langkah yang dilakukan untuk memperoleh pengetahuan ilmiah atau sistematis. Metode penelitian merupakan cara sistematis dengan metode ilmiah

untuk menyusun ilmu pengetahuan. Teknik penelitian adalah cara untuk melaksanakan metode penelitian. Metode penelitian biasanya mengacu pada bentuk-bentuk penelitian. Dalam penelitian ini terdapat beberapa metode yaitu :

1. Teknik Pengumpulan Data (Collecting Data)

Adapun beberapa teknik yang digunakan dalam pengumpulan data dari penelitian ini yaitu :

a. Pengamatan (Observasi)

Observasi merupakan teknik pengumpulan data yang dilakukan dengan tinjauan langsung ketempat studi kasus, dimana akan dilakukan penelitian. Dalam hal ini dilakukan observasi di PT.Dayamega Pratama Medan. Pada toko tersebut dilakukan analisis secara langsung setiap harinya sebagai sumber data. Data yang digunakan dalam penelitian ini adalah data primer dan sekunder yang merupakan data yang diperoleh secara langsung dari PT.Dayamega Pratama Medan.

Tabel 3.1 Data Serial Number Product

No	Nama Barang	Part Number	Serial Number
1	Lenovo AIO A340-22IWL	FOEB000PID	MP1N1XK4
2	Lenovo S340-14API	81NB00BTID	MP1PHGCJ
3	Lenovo IP130-14AST	81H40000ID	MP1NDJN4
4	Lenovo AIO A340-24ICK	FOER008FID	MP1NCBP8
5	Lenovo AIO V130-20IGM	10RX002JID	YJ00ZHCK
6	Lenovo AIO V530-22ICB	10US00LSIA	MP1FX8C0
7	Lenovo Legion 5	82B5002WID	PF28ZJ2J
8	Lenovo AIO A340-24ICK	FOER0079ID	MP1NAS0F
9	Lenovo IP S145-14IWL	81MU00TAID	PF1V31PX
10	Lenovo Yoga C640-13IML	81UE0033ID	LR0D2RK6

b. Wawancara (Interview)

Teknik wawancara dilakukan kepada pihak-pihak yang terlibat dalam rekrutmen pegawai serta mewawancarai mereka dan menanyakan tentang apa yang menjadi masalah selama ini. Pihak yang terkait adalah pegawai di bidang penerimaan barang/produk masuk ke PT.Dayamega Pratama Medan.

2. Studi Literatur

Untuk mendapatkan studi literatur yang valid, untuk dijadikan suatu landasan dapat mempelajari beberapa buku referensi. Dan untuk menguatkan landasan pemikiran didalam pemecahan masalah digunakan dengan beberapa jurnal Nasional yang sesuai melalui internet serta buku-buku.

**3.2 Metode Perancangan Sistem**

Metodologi Perancangan Sistem adalah suatu tahapan yang harus dilakukan setelah menganalisis sebuah masalah, pada tahapan inilah perancangan sebuah sistem direncanakan. Salah satu cara dalam merancang atau membangun sebuah sistem adalah dengan menggunakan Metode Waterfall.

Metode Waterfall adalah model yang menyediakan pendekatan alur hidup perangkat lunak secara sekuensial terurut dimulai dari analisis, desain, pengkodean, pengujian dan tahap pendukung (support). Sesuai dengan rumusan masalah yang menggunakan pendekatan Classic or Waterfall Algorithm maka berikut ini adalah teknik perancangan sistem yang digunakan:

a. Analisis Masalah dan Kebutuhan

Pada tahapan Analisis Masalah dan Kebutuhan, dilakukan dengan penelitian, wawancara ke PT. Dayamega Pratama Medan. Dimana penelitian pada tahap ini dilakukan dengan cara mencari permasalahan dan persoalan tentang data serial number atau nomor seri yang ingin diamankan.

b. Perancangan Sistem dan Pemodelan

Tahap Perancangan dan Pemodelan berfokus pada struktur data, arsitektur perangkat lunak, representasi interface, dan detail (algoritma) prosedural. Pada tahapan ini diran tampilan program dan database yang akan digunakan pada sistem. Yang sebelumnya telah dim  
dengan menggunakan Unified Modelling Language (UML).

c. Pengkodean

Pengkodean dilakukan dengan menterjemahkan hasil dari Perancangan dan Pemodelan ke dalam bahasa pemrograman berbasis Desktop Programming agar dikenali oleh komputer agar menjadi suatu sistem yang menjadi solusi dari permasalahan untuk mengamankan data nomor seri dengan menggunakan model Merkle Hellman.

d. Percobaan Awal

Melakukan pengujian program atau sistem yang telah dikodekan agar mengetahui bug-bug yang ada pada program atau sistem yang telah dirancang agar diperoleh sistem yang berjalan sesuai dengan yang telah dirancang sebelumnya. Pada tahapan ini, program atau sistem yang telah dibangun akan diuji coba sendiri, kemudian melihat setiap detail program apakah berjalan sesuai dengan yang telah dirancang atau masih ada kesalahan.

e. Percobaan Akhir

Pada tahapan percobaan akhir, sistem yang telah melalui tahapan Percobaan Awal akan diterapkan pada user dan dilakukan pengujian oleh user. Dalam tahap ini ditinjau pula apakah program sudah layak untuk digunakan pada PT. Dayamega Pratama Medan.

### 3.3 Algoritma Sistem

Algoritma Sistem merupakan langkah-langkah yang dilakukan sebuah sistem dalam memproses dan menyelesaikan suatu permasalahan. Berikut ini adalah flowchart atau alur dari pemecahan permasalahan dengan menggunakan metode Merkle Hellman.

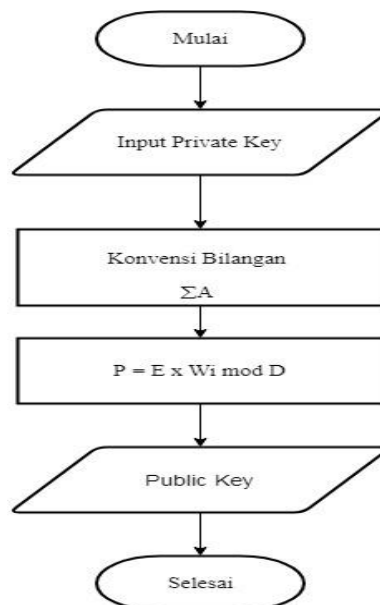
#### 3.3.1 Penerapan Metode Merkle Hellman

Adapun penerapan algoritma sistem dalam permasalahan ini menggunakan metode Merkle Hellman adalah sebagai berikut :

1. Membuat Private key (S, A, dan P).
2. Membuat Public Key .
3. Mengubah Plaintext ke biner.
4. Menjumlahkan (perkalian biner dengan Publik key).
5. Mengurangkan data dengan nilai S.

#### 3.3.2 Perancangan Flowchart Pembentuk Kunci

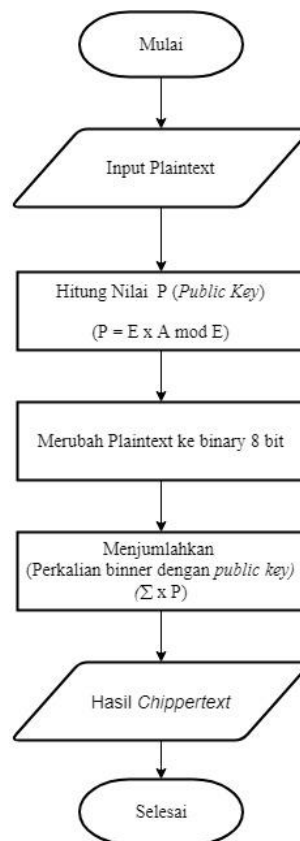
Flowchart pembentukan kunci merupakan penjelasan yang lebih jelas, dan teliti.dalam pembentuk kunci pada program algoritma Merkle Hellman sebagai berikut :



Gambar 3.1 Flowchart Pembentukan Public Key

#### 3.3.2 Perancangan Flowchart Enkripsi

*Flowchart* Enkripsi merupakan penjelasan yang lebih jelas, dan teliti.dalam Enkripsi pada program algoritma Markle Hellman sebagai berikut :



**Gambar 3.2** *Flowchart* Enkripsi Algoritma Sistem

### 3.3.3 Perancangan *Flowchart* Dekripsi

*Flowchart* dekripsi adalah proses mengembalikan data rahasia menjadi data asli. Proses ini dilakukan agar dapat membaca data yang telah di enkripsi sebelumnya. *Flowchart* dekripsi pada metode Merkle Hellman adalah sebagai berikut :



Gambar 3.3 Flowchart Dekripsi Algoritma Sistem

### 3.3.4 Membuat *Private Key* (S, A dan P)

$$S = (2,4,7,14,28,112,224,407) = \sum s = 798$$

$$A = 989$$

$$P = 578$$

### 3.3.5 Membuat *Public Key*

Plaintext (x) : MP1NCBP8

Enkripsi :

Perhitungan *Public Key* (T) :

$$T = P \times S_i \text{ mod } A$$

$$T1 = 578 \times 2 \text{ mod } 989 = 167$$

$$T2 = 578 \times 4 \text{ mod } 989 = 334$$

$$T3 = 578 \times 7 \text{ mod } 989 = 90$$

$$T4 = 578 \times 14 \text{ mod } 989 = 180$$

$$T5 = 578 \times 28 \text{ mod } 989 = 360$$

$$T6 = 578 \times 112 \text{ mod } 989 = 451$$

$$T7 = 578 \times 224 \text{ mod } 989 = 902$$

$$T8 = 578 \times 407 \text{ mod } 989 = 853$$

Didapatkan

$$T = (167,334,90,180,360,451,902,853)$$

### 3.3.6 Mengubah Plaintext ke Biner 8 Digit

Pada Proses ini data perlu diubah menjadi bentuk biner karena perhitungan *Merkle Hellman* menggunakan teknik binary sebagai proses enkripsi dan dekripsinya

Plaintext : MP1NCBP8

Dimasukkan kedalam kode ASCII

$$X = 77 \quad 80 \quad 49 \quad 78 \quad 67 \quad 66 \quad 80 \quad 56$$

Masing-masing kode ASCII kemudian di konversi ke biner.

Tabel 3.2 Data Binary

Plaintext	ASCII	Binary(Z)
M	77	01001101
P	80	01010000
1	49	00110001
N	78	01001110
C	67	01000011
B	66	01000010
P	80	01010000
8	56	00111000

### 3.3.7 Menjumlahkan (Perkalian biner dengan Public key).

Plaintext dibagi dalam blok sesuai dengan banyaknya S, pada contoh ini banyaknya S adalah 8 digit

$$\begin{aligned}
 01001101 &= (0x167)+(1x334)+(0x90)+(0x180)+(1x360)+(1x451)+(0x902) \\
 + (1x853) &= 1998 \\
 01010000 &= (0x167)+(1x334)+(0x90)+(1x180)+(0x360)+(0x451)+(0x902) \\
 + (0x853) &= 514 \\
 00110001 &= (0x167)+(0x334)+(1x90)+(1x180)+(0x360)+(0x451)+(0x902) \\
 + (1x853) &= 1123 \\
 01001110 &= (0x167)+(1x334)+(0x90)+(0x180)+(1x360)+(1x451)+(1x902) \\
 + (0x853) &= 2047 \\
 01000011 &= (0x167)+(1x334)+(0x90)+(0x180)+(0x360)+(0x451)+(1x902) \\
 + (1x853) &= 2089 \\
 01000010 &= (0x167)+(1x334)+(0x90)+(0x180)+(0x360)+(0x451)+(1x902) \\
 + (0x853) &= 1236 \\
 01010000 &= (0x167)+(1x334)+(0x90)+(1x180)+(0x360)+(0x451)+(0x902) \\
 + (0x853) &= 514 \\
 00111000 &= (0x167)+(0x334)+(1x90)+(1x180)+(1x360)+(0x451)+(0x902) \\
 + (0x853) &= 630
 \end{aligned}$$

Ciphertext:

$$1998 \quad 514 \quad 1123 \quad 2047 \quad 2089 \quad 1236 \quad 514 \quad 630$$

### 3.3.8 Mengubah Chiphertext ke Plaintext (Dekripsi)

Langkah-langkah dalam proses dekripsi dengan menggunakan metode *Merkle Hellman* adalah sebagai berikut:

1. Data *Chiphertext* (O)

Dalam melakukan proses dekripsi, terlebih dahulu harus ada data yang lengkap dari proses enkripsi. Selain itu diperlukan juga *private key* sebagai kunci untuk proses dekripsi data.

Kode *Chiphertext* adalah sebagai berikut:

C{1998 514 1123 2047 2089 1236 514 630}

2. Modular *Invers*

Proses untuk mencari nilai modular invers dari (p-1) dengan menggunakan metode *extended euclidian*, yaitu ( $P \times M \text{ mod } A = 1$ ). Dalam proses dekripsi ini akan digunakan nilai p-1 sebesar 77. Nilai 77 diperoleh dari hasil perhitungan menggunakan metode *extended euclidian*, seperti tabel di bawah ini:

Tabel 3.3 Modular *Invers*

M	PxM mod A	
1	$578 \times 1 \text{ mod } 989$	578
2	$578 \times 2 \text{ mod } 989$	167
3	$578 \times 3 \text{ mod } 989$	745
.....	$..... \times ... \text{ mod } .....$	.....
77	$578 \times 77 \text{ mod } 989$	1

3. *Chipper Data Mod A*

Proses berikutnya adalah proses mod, yaitu untuk data *chiphertext* dengan nilai *invers* yang diperoleh sebelumnya.

Tabel 3.4 Data Mod A

O	M	(O x M) Mod A	
1998	77	$514 \times 77 \text{ mod } 989$	551
514	77	$1236 \times 77 \text{ mod } 989$	18
1123	77	$1123 \times 77 \text{ mod } 989$	428
2047	77	$2047 \times 77 \text{ mod } 989$	368
2089	77	$2089 \times 77 \text{ mod } 989$	635
1236	77	$1236 \times 77 \text{ mod } 989$	228



		989	
514	77	$514 \times 77 \text{ mod } 989$	18
630	77	$630 \times 77 \text{ mod } 989$	49

4. Mengurangkan Data dengan Nilai S

Proses Pengurangan data (K) dengan nilai-nilai pada elemen S. Pengurangan terus dilakukan dari elemen data 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*.

$$S = \{2, 4, 7, 14, 28, 112, 224, 407\}$$

$$K = \{551, 18, 428, 368, 635, 228, 18, 49\}$$

Setelah semua proses pengurangan data dengan nilai s telah selesai maka *plaintext* dimasukkan ke dalam kode ASCII maka akan didapatkan hasil seperti pada tabel berikut :

Tabel 3.5 Data *Plaintext*

Binary(Z)	ASCII	Plaintext
01001101	77	M
01010000	80	P
00110001	49	1
01001110	78	N
01000011	67	C
01000010	66	B
01010000	80	P
00111000	56	8

Maka dapat disimpulkan bahwa proses dekripsi telah berhasil karena hasil akhir perhitungan telah kembali ke *plaintext* yaitu : “MP1NCBP8”.

5. Kesimpulan

Setelah melalui proses penyelesaian tugas akhir (skripsi) yang berjudul "Security Serial Number Product pada PT. Dayamega Pratama Medan dengan Menggunakan Metode Merkle Hellman" penulis mengambil kesimpulan sebagai berikut:

1. Keunggulan dari metode Merkle Hellman mempunyai keamanan yang kuat dengan jumlah kunci yang lebih banyak dibanding dengan kriptosistem seperti RSA.
2. Berdasarkan uji coba yang telah dilakukan, aplikasi ini berhasil mengimplementasikan proses

enkripsi dan dekripsi untuk mengamankan data. Hal ini dibuktikan melalui pengujian yang telah

dilakukan bahwa semua data yang telah di enkripsi dapat dikembalikan ke bentuk semula dalam proses dekripsi dan data tidak mengalami perubahan.

3. Aplikasi yang telah dirancang dapat menghitung atau mengolah (enkripsi dan dekripsi) dengan cepat.

4. Aplikasi ini dapat dengan mudah digunakan karena rancangan Interface yang sederhana.

## UCAPAN TERIMA KASIH

Terimakasih kepada Ketua Yayasan STMIK Triguna Dharma, kepada Bapak Azanuddin S.Kom., M.Kom selaku dosen pembimbing I, kepada Bapak Jufri Halim, S.E., M.M selaku dosen pembimbing II, kepada kedua orang tua, saudara saya yang selalu memberi dukungan dan teman seperjuangan. Kiranya jurnal ini bisa memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

## REFERENSI

- [1] W. Wardiana and P. Informatika-lipi, "Pencegah Pembajakan Perangkat Lunak dengan Menggunakan Teknik Identity-Based Encryption dan Obfuscation," *Pencegah Pembajakan Perangkat Lunak dengan Menggunakan Tek. Identity-Based Encryption dan Obfuscation*, vol. III, no. 1, pp. 97–104, 2009, [Online]. Available: [https://www.mendeley.com/research-papers/pencegah-pembajakan-perangkat-lunak-dengan-menggunakan-teknik-identitybased-encryption-dan-obfuscation/?utm\\_source=desktop&utm\\_medium=1.17.11&utm\\_campaign=open\\_catalog&userDocumentId=%7B3bfffcc30-143f-4818-a15e-0207c7](https://www.mendeley.com/research-papers/pencegah-pembajakan-perangkat-lunak-dengan-menggunakan-teknik-identitybased-encryption-dan-obfuscation/?utm_source=desktop&utm_medium=1.17.11&utm_campaign=open_catalog&userDocumentId=%7B3bfffcc30-143f-4818-a15e-0207c7).
- [2] L. Nisa, T. Indriyani, and M. Ruswiansari, "Aplikasi Enkripsi Citra dan Teks Menggunakan Algoritma Diffie-Hellman dan ElGamal," *J. Teknol. dan Manaj.*, vol. 1, no. 1, pp. 8–17, 2020.
- [3] A. Hidayat, Akmal, and R. Rosyadi, "Cryptography Asymmetries Merkle-Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks," *Sumedang Univ. Pdjadjaran*, pp. 27–28, 2016, [Online]. Available: <http://riset.fmipa.unpad.ac.id/data/uploads/paper/semnas/2016/014.-066-068-akik-hidayat.pdf>.
- [4] S. Of, G. Information, S. Readiness, and I. N. Implementing, "DALAM PENERAPAN E-GOVERNMENT," pp. 109–126, 2013.
- [5] T. D. U. M. Buana, "Kripto grafi," p. 206, 2010.
- [6] D. Andriani, "Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining," *J. Tek. Inform. Unika St. Thomas*, vol. 02, no. 338, pp. 14–23, 2017.
- [7] D. Mukodim, "Tinjauan Tentang Enkripsi dan Dekripsi, Suatu Teknik Pengamanan Data dengan Penyandian RSA," *Komput. dan Sist. Intelijen*, pp. 92–100, 2002.
- [8] O. W. Purbo and T. Wiharjito, *Keamanan Jaringan Internet*. Jakarta, 2000.
- [9] A. D. Nugroho, I. T. Bandung, and J. G. Bandung, "Penggabungan Algoritma Kriptografi Simetris dan Kriptografi Asimetris untuk Pengamanan Pesan," no. 13511051, 2015.
- [10] D. Email, A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk," vol. 3, no. 2, pp. 253–258, 2015.
- [11] I. Gunawan, "Keamanan Data : Teori dan Implementasi," no. January, 2020.
- [12] Suendri, "Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan)," *J. Ilmu Komput. dan Inform.*, vol. 3, no. 1, pp. 1–9, 2018, [Online]. Available: <http://jurnal.uinsu.ac.id/index.php/algoritma/article/download/3148/1871>.
- [13] E. F. Wati and A. A. Kusumo, "Penerapan metode unified modeling language ( UML ) berbasis desktop pada sistem pengolahan kas kecil studi kasus pada PT indo mada yasa tangerang," *J. Inform.*, vol. 5, no. 1, pp. 24–36, 2016, [Online]. Available: <https://journal.unsika.ac.id/index.php/syntax/article/view/699>.
- [14] M. S. Rosa, *Rekayasa Perangkat Lunak*. Bandung, 2014.

- [15] A. Hendini, "Pemodelan Uml Sistem Informasi Monitoring Penjualan Dan Stok Barang," J. Chem. Inf. Model., vol. 53, no. 9, pp. 1689–1699, 2013, doi: 10.1017/CBO9781107415324.004.

**Bibliografi Penulis**

	<p><b>Data Diri</b></p> <p>Nama : Agnes Synthya Rg Tempat/Tanggal Lahir : Medan, 08 Februari 1998 Jenis Kelamin : Perempuan Agama : Kristen Protestan Status : Belum Menikah Pendidikan Terakhir : Sekolah Menengah Kejuruan Kewarganegaraan : Indonesia E-mail : agnessynthya8@gmail.com</p> <p><b>Pendidikan Formal</b></p> <p>Tahun 2003 - 2007 : SD NEGERI 068008 MEDAN Tahun 2007 - 2009 : SD NEGERI 064990 MEDAN Tahun 2009 -2012 : SMP NEGERI 10 MEDAN Tahun 2012 -2015 : SMK NEGERI 7 MEDAN</p>
	<p><b>Azanuddin, S.Kom., M.Kom</b> Beliau merupakan Ketua Prodi Manajemen Informatika di STMIK TRIGUNA DHARMA</p>
	<p><b>Jufri Halim, S.E., M.M</b> Beliau merupakan dosen pengajar tetap di STMIK TRIGUNA DHARMA</p>