Jurnal CyberTech
Vol.1. No.2, Mei 2018, pp. 438~447
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Kriptografi Untuk Mengamankan Data Nilai Menggunakan Metode Merkle Hellman

Nur Septiani[*], Badrul Anwar[**], Sobirin
[*] Program Studi Mahasiswa, STMIK Triguna Dharma
[**] Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info
Article history:

Received Mei 12th, 2018
Revised Mei 20th, 2018
Accepted Mei 26th, 2018

Keyword:
Pengamanan,
Kriptografi, Merkle Hellman.

ABSTRACT
Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data dan informasi di suatu instansi. Pada Sekolah SMK Negeri 1 Beringin terdapat data nilai-nilai siswa yang bersifat rahasia. Seringkali dengan diketahuinya data dan informasi pada data nilai siswa dijadikan celah untuk pihak yang tidak berwenang untuk merusak dan mengubah bahkan menghilangkan data. Dengan berkembang pesatnya teknologi informasi komputer kerahasiaan data dapat diminimilalisir dengan ilmu Kriptografi. Kriptografi merupakan metode dengan menyandikan isi informasi (plaintext) menjadi isi yang sulit atau bahkan tidak bisa dipahami melalui proses enkripsi yang kemudian di dekripsi. Dalam keamanan data ini metode yang digunakan adalah Metode Merkle Hellman. Perancangan program aplikasi Pengamanan Data Nilai Siswa SMK Negeri 1 Beringin menggunakan metode Merkle Hellman akan menghasilkan sebuah sistem keamanan yang lebih terjamin sebagai rekomendasi untuk mengamankan data nilai siswa.

First Author
Nama : Nur Septiani
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : Nurseptiyani@gmail.com

1. PENDAHULUAN

Sekolah SMK ada yang dikelola oleh pemerintah dan ada juga yang dikelola oleh swasta. Salah satu SMK yang dikelola oleh pemerintah adalah SMK Negeri 1 Beringin, SMK Negeri 1 Beringin saat ini memiliki 7 jurusan. SMK Negeri 1 Beringin setiap tahunnya banyak meluluskan siswa dengan jalur SNMPTN dengan berdasarkan nilai yang diperoleh siswa sejak kelas X hingga kelas XII di SMK Negeri 1 Beringin. Karena yang menjadi syarat dari kelulusan adalah nilai, maka ada kekhawatiran terhadap nilai-nilai siswa ini bisa dimanipulasi atau diubah. Karena selama ini media penyimpanan nilai USBN siswa masih terlalu sederhana dan masih menggunakan Ms. Excell. Dengan jumlah siswa yang mencapai 104 orang, itu perlu ditingkatkan lagi keamanan data nilai tersebut. Seiring dengan majunya teknologi saat ini, merupakan salah satu masalah yang harus diatasi oleh SMK Negeri 1 Beringin agar nilai-nilai siswa tetap asli dan tidak dimanipulasi.cara manual.

Dari pembahasan penelitian tersebut diharapkan *software* yang dirancang dapat membantu pihak sekolah dalam mengamankan data nilai siswa, dengan adanya aplikasi ini dapat membantu mengamankan data nilai siswa pada SMK Negeri 1 Beringin Kecamatan Beringin menggunakan kunci Asimetris. Berdasarkan deskripsi masalah diatas maka dilakukan penelitian skripsi dengan judul **"Implementasi Kriptografi Untuk Mengamankan Data Nilai Pada SMK Negeri 1 Beringin Menggunakan Metode Merkle Hellman."**

2. METODE PENELITIAN

2.1 Kriptografi

Suatu implementasi kriptografi merupakan sistem yang dibuat untuk membantu mengamankan permasalahan tersebut.

2.2 Tujuan Kriptografi

Tujuan kriptografi agar dapat mengamankan suatu data.

1. Membantu mengamankan data nilai pada smk negeri 1 beringin.
2. Mengamankan suatu data nilai agar tidak dapat dimanipulasi.
3. Meningkatkan efektivitas keamanan data nilai sekolah tersebut.

2.3 Metode *KRIPTOGRAFI*

Kriptografi berasal dari Bahasa Yunani, yaitu *cryptho* dan *graphia. Cryptho* artinya *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari satu tempat ke tempat yang lain.(Dony Ariyus, 2008 : 13).

Menurut Bruce Schneier (dalam Ripanti dan Maulana, 2006 : 49) 'Kriptografi adalah seni dan ilmu untuk menjaga agar pesan rahasia tetap aman. Kriptografi merupakan salah satu cabang ilmu algoritma matematika'.

Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas.(Rifki Sadikin, 2012).

2.3.1 Konsep Dasar Penggunaan Metode Merkle Hellman

Berikut ini adalah algoritma penyelesaian metode Merkle Hellman yaitu sebagai berikut:

1. Langkah Pertama : Algoritma simetrik dapat disebut sebagai algoritma konvensional, dimana kunci dekripsi dapat ditentukan dari kunci enkripsinya, begitu pula sebaliknya. Pada algoritma ini, knci enkripsi dan dekripsinya sama.
2. Langkah Kedua : Algoritma Asimetrik (*Asymmetric* atau *Public key*) adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Algoritma ini disebut juga algoritma kunci umum (*public keyalgorithm*) karena kunci untuk enkripsi dibuat umum atau dapat diketahui setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan.

Contoh Kasus

2.3.2 Pengamanan Data

Metode MERKLE HELLMAN dalam prosesnya memerlukan data yang akan dijadikan bahan perhitungan. Nilai A, N, Y adalah sebuah variable untuk private key, bilangan bulat yang disusun dengan algoritma superincreasing linier. A adalah bilangan bulat positif yang dipilih dari bilangan terkecil, lalu pilih bilangan berikutnya lebih besar dari pada bilangan sebelumnya, kemudian pilih bilangan yang lebih besar dari pada penjumlahan bilangan pertama dan kedua, teruskan proses pemilihan bilangan-bilangan lebih besar dari semua penjumlahan bilangan sebelumnya dipilih. N adalah nilai atau angka bebas yang harus lebih besar dari jumlah keseluruhan nilai A. Y adalah nilai atau angka bebas relatif prima N dimulai dari angka 1 sampai dengan nilai atau angka lebih kecil dari nilai atau angka N.

Tabel 2.2 Private Key

A	{3,5,9,18,36,78,171,340}= ∑A = 660
N	860
Y	449

Plaintext : **90 = 1011010**

Tabel 2.3 Public Key

A	**P = (Y * Ai) mod N**	
3	449 * 3 mod 860	487
5	449 * 5 mod 860	525
9	449 * 9 mod 860	601
18	449 * 18 mod 860	342
36	449 * 36 mod 860	684

78	449 * 78 mod 860	622
171	449 * 171 mod 860	239
340	449 * 340 mod 860	440

Kunci publik untuk proses *enkripsi* ini sebagai berikut :
{487,525,601,342,684,622,239,440}.

Tabel 2.4 Data Binnary

Plaintext	ASCII	Binnary
9	57	0011 1001
0	48	0011 0000

Tabel 2.5 Proses Perhitungan Data Chippertext

Binary (z)	∑z * P	Chippertext
0011 1001	(0 *487)+(0*525)+(1*601)+(1*342)+(1*684)+(0*622)+(0*239)+(1 *440)	2067
0011 0000	(0 *487)+(0*525)+(1*601)+(1*342)+(0*684)+(0*622)+(0*239)+(0 *440)	943

Proses Dekripsi

Tabel 2.6 Modular *Invers*

M	(Y * M) mod N	
1	449 * 1 mod 860	449
2	449 * 2 mod 860	38
3	449 * 3 mod 860	487
…	…	…
249	449 * 249 mod 860	1

Tabel 2.7 Cipher Data Mod M

Chipper (C)	M	K = (C * M) mod N	
2067	249	2067 * 249 mod 860	403
943	249	943*249 mod 860	27

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 superincreasing linier. 90 = {3,5,9,18,36,78,171,340 }, K = {403,27}

Tabel 2.8 Chipper Data Mod Q

3	5	9	18	36	78	171	340	S
							403-340	K
						63-171	= 63	
					63-78			
				63-36				
			27-18	= 27				
		9-9	= 9					
	0-5	= 0						
0-3								
0	0	1	1	1	0	0	1	

Proses perhitungan pada tabel diatas dimulai dari kanan ke kiri, kolom yang diberi tanda *false* berarti pada elemen S kolom tersebut data tidak dapat dikurangkan 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 "00111001" yang apabila dikembalikan ke kode decimal menjadi "57" dank e *char* menjadi "9". Proses berikutnya, nilai V1 sampai V2 akan didekomposisi menggunakan setiap nilai pada S. Dekomposisi ini dilakukan dengan cara pengurangan terhadap nilai terbesar sampai terkecil dan menghasilkan nilai Vi=0.

- V1 = 403 – 340 = 63 (1) | 63 – 171 = 63(0) | 63 – 78 = 63(0) | 63 – 36 = 27(1) | 27 – 18 = 9(1) | 9 – 9 = 0(1) | 0 – 5 = 0(0) | 0 – 2 = 0(0)

Maka diperoleh hasil = 00111001

- V2 = 27 – 340 = 27(0) | 27 – 171 = 27(0) | 27 – 78 = 27(0) | 27 – 36 = 27(0) | 27 – 18 = 9(1) | 9 – 9 = 0(1) | 0 – 5 = 0(0) | 0 – 3 = 0(0)

Maka diperoleh hasil = 00110000

Z = {00111001, 00110000}

Mengembalikan ke Data Asli

Mengembalikan ke data asli adalah tahapan terakhir untuk menkonversi ke proses dekripsi. Adapun kode *binary* disusun dan dikonversi ke kode decimal lalu ke kode *char*.

C = C{2067,943}

Z = {90}

3.3.1 Pengujian

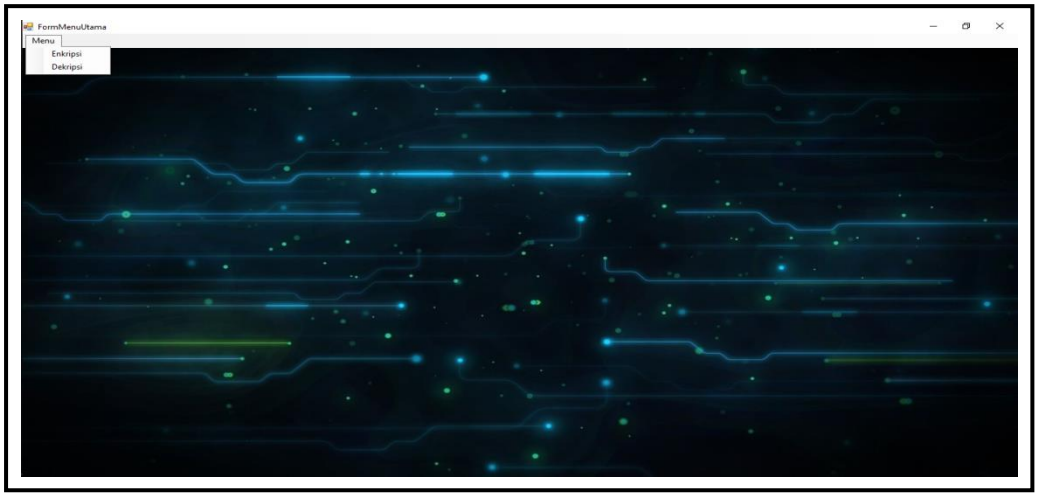
1. *Form Login*

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 4.1 Tampilan *Form Login*

3.1.2 *Form* Menu Utama

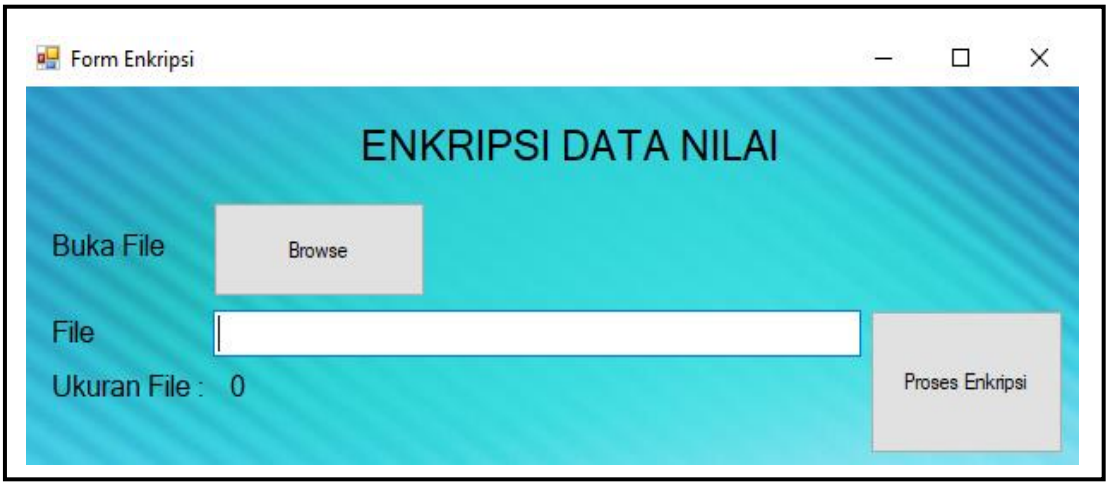
Form menu utama adalah tampilan navigasi. Di mana di dalamnya terdapat menu-menu untuk membuka *form* lainnya.



Gambar 4.2 Tampilan menu utama

3.1.3 *Form* Enkripsi

Form enkripsi dibawah ini digunakan untuk melakukan proses enkripsi atau penyandian terhadap *file* yang telah di *import* di *form* enkripsi berupa data *Microsoft excel.*



Gambar 4.3 Tampilan *Form* Enkripsi

3.1.4 *Form* Dekripsi

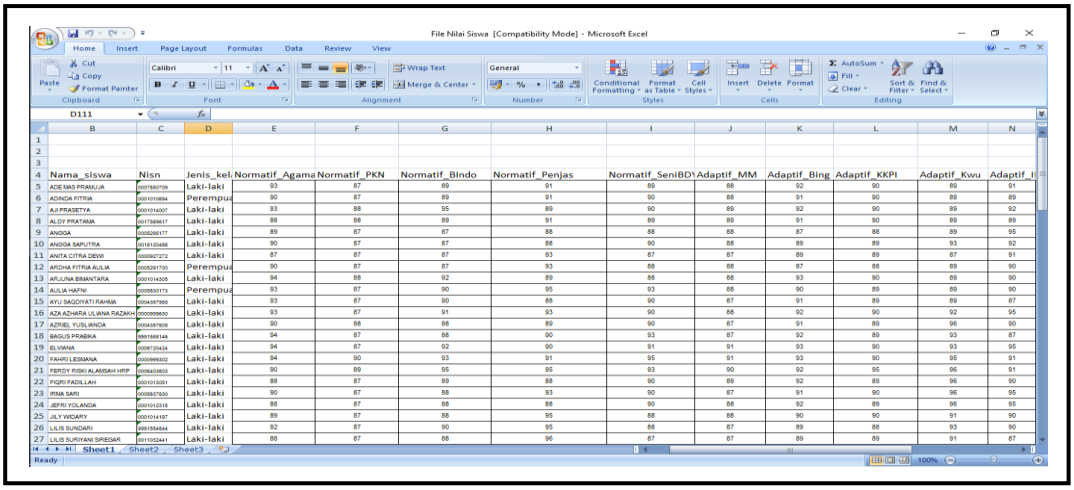
Form dekripsi dibawah ini digunakan untuk melakukan proses pengembalian data yang telah dilakukan proses enkripsi

Gambar 4.4 Tampilan *Form* Dekripsi

3.1.5 Pengujian

Setelah melakukan proses implementasi, proses selanjutnya adalah uji coba dengan mengetahui bahwa hasil perancangan di bab III 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.

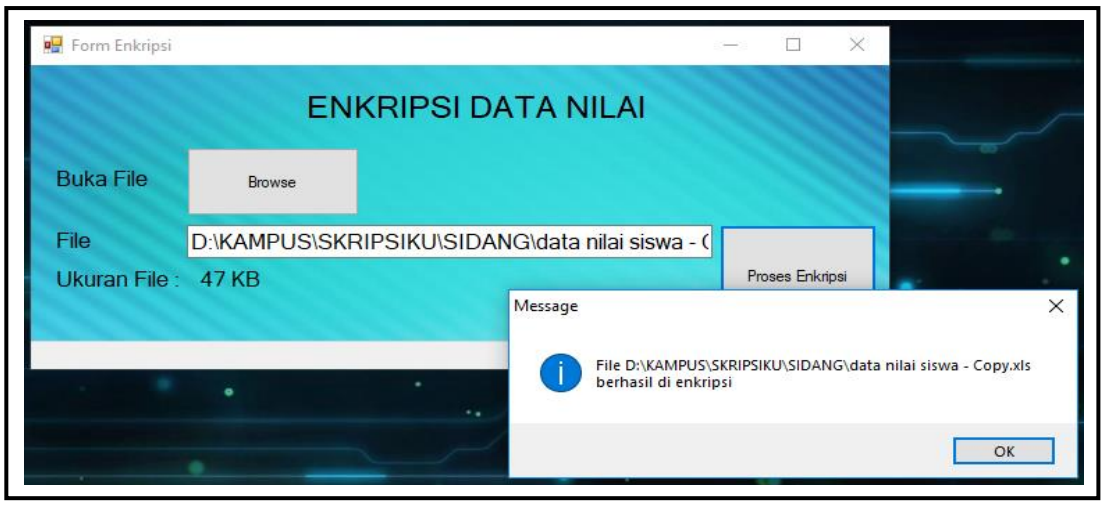
File yang akan di enkripsi adalah *file* nilai siswa dalam bentuk *excel*, adapun data nilai tersebut adalah sebagai berikut :



Gambar 4.5 Tampilan Awal Data Nilai Siswa

3.1.6 *Form* Enkripsi

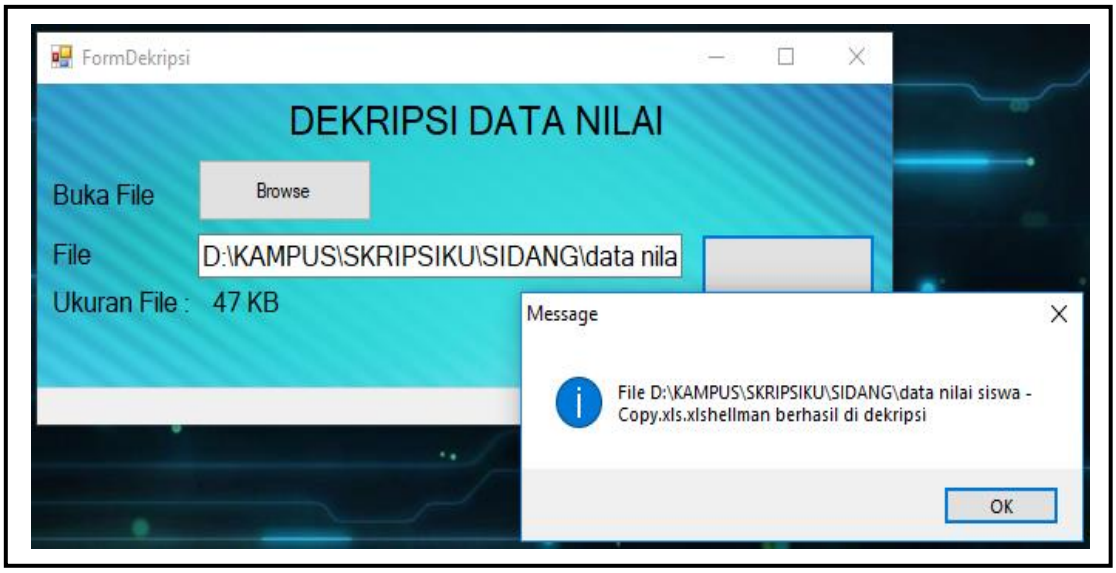
Berikut melakukan enkripsi terhadap data nilai tersebut



Gambar 4.6 Tampilan Proses Enkripsi Data Nilai Siswa

3.1.7 *Form* Dekripsi

Berikut melakukan dekripsi terhadap data nilai tersebut



Gambar 4.7 Tampilan Proses Dekripsi Pada Nilai Siswa

4 KESIMPULAN

Kesimpulan yang terdapat dari proses kriptografi untuk pengamanan data nilai siswa pada SMK Negeri 1 Beringin bahwa metode *Merkle Hellman* yaitu :

1. Metode *Merkle Hellman* dapat digunakan untuk mengamankan data nilai siswa sehingga privasi tentang data nilai siswa di SMK Negeri 1 Beringin aman sehingga data tidak jatuh ke pihak ke tiga.
2. Rancangan kriptografi ini memiliki tingkat keamanan yang baik dikarenakan memiliki dua kunci pengamanan yaitu *public key* dan *private key.*
3. Aplikasi yang dirancang dapat dijadikan sebagai pemecahan masalah dalam hal keamanan data nilai siswa pada SMK Negeri 1 Beringin.
4. Rancangan penyandian data dibuat sesuai dengan kebutuhan pihak SMK Negeri 1 Beringin.

5. Saran

Agar sistem keamanan data nilai siswa dengan menggunakan metode *Merkle Hellman* semakin baik, ada beberapa saran untuk digunakan pada penelitian selanjutnya yaitu:

1. Aplikasi keamanan data nilai siswa pada SMK Negeri 1 Beringin yang dibuat masih terbatas pada data berupa excel, sehingga disarankan untuk mengembangkan aplikasi ini agar bisa digunakan pada data dengan format yang lainnya seperti Gambar, Suara, Video dan lain-lain.
2. Aplikasi keamanan data sebaiknya kunci antara enkripsi dan dekripsi harus di kembangkan sehingga tidak terjadinya error pada kondisi tertentu dikarenakan tidak sesuainya antara *private key* dan *public key*.
3. Aplikasi keamanan data yang dirancang berbasis *Desktop*, diharapkan dapat dikembangkan dalam bentuk aplikasi berbasis web atau android agar bisa di akses secara online.
4. Sistem kriptografi ini hanya mampu memberikan pengamanan terhadap data yang terdapat di excel saja, alangkah baiknya dikembangkan untuk jenis file lainnya.

DAFTAR PUSTAKA

A, N. R. D. P. (1997). Perancangan Modifikasi Kriptografi Modern CBC untuk Pengamanan Data/File Text, 1-8.

Ariyus, Dony. *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi, 2008.

Fadlan, M., &Hadriansa. (2017). Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher, *4*(4), 268–274.

Mardalius. (2018). IMPLEMENTASI APLIKASI ENKRIPSI DAN DEKRIPSI TEXT PADA VISUAL BASIC . NET MENGUNAKAN ALGORITMA MERKLE HELLMAN KNAPSACK, *249-252*.

Munawar 2018. *Analisis Perancangan Sistem Berorientasi Objek dengan UML.* Bandung: Informatika Bandung.

Murdani. (2017). PERANCANGAN APLIKASI KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA MERKLE HELLMAN KNAPSACK, *16*, 302–305.

Rosdiana., ST., & Kom, M. (n.d.). SEKURITAS SISTEM DENGAN KRIPTOGRAFI, 21–32.

Rossa A.S., & Shalahuddin, M. 2015. *Rekayasa Perangkat Lunak dan Berorientasi Objek.* Bandung: Informatika

Bandung.

BIOGRAFI PENULIS

Nur Septiani, Kelahiran Lubuk Pakam, 23 September 1997 anak ketiga dari lima bersaudara.
Anak dari Bapak Muhammad Husni dan Ibu Rosmaida Samosir S.Pd

	**Badrul Anwar, S.E., S.Kom., M.Kom,** Beliau merupakan dosen tetap STMIK Triguna Dharma, Beliau aktif sebagai dosen khususnya pada bidang Sistem Informasi.
	**Drs. Sobirin, SH., M.Si**.merupakan dosen tetap STMIK Triguna Dharma, Beliau aktif sebagai dosen khususnya pada bidang Sistem Informasi.