Cyber Tech
Vol. . No. , Agustus 2020, pp.
E-ISSN: 13-08-2020

"Implementasi Kriptografi dalam Pengamanan Data Laba Penjualan pada PT. Efata Indonesia Tour & Travel dengan Metode Merkle Hellman"

Herman Efendi, Faizal Taufik, S.Kom., M.Kom, Devri Suherdi, S.Kom., M.Kom
[#1]Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:

Keyword:
Kriptografi Pengamanan Data Laba Penjualan

ABSTRACT

Data laba penjualan merupakan data yang menyimpan arsip tentang laba bersih (net profit) yang telah dikurangi biaya-biaya yang menjadi beban perusahaan dalam suatu periode tertentu termasuk pajak. Penjualan dan laba pada perusahaan merupakan suatu hal yang sifatnya internal dan tidak semua pihak boleh mengetahuinya, keuntungan yang diperoleh perusahaan tidak akan dibocorkan termasuk kepada karyawan, terkecuali pada karyawan bagaian keuangan.

Berkembangnya cabang ilmu yang mempelajari tentang cara-cara pengamanan data merupakan dampak positif dari tuntutan tersedianya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi. Kriptografi merupakan ilmu yang mempelajari tehnik-tehnik matematika yang berhubungan dengan aspek keamanan data dan informasi seperti keabsahan data, integritas data, serta autentifikasi data. Sistem keamanan data yang akan di bangun berbasis desktop dan menggunakan Algoritma Markle Hellman.

Dengan membangun sistem Algoritma Markle Hellman diharapkan dapat membantu perusahaan dalam mengamankan data laba penjualan secara baik, aman dan cepat, sehingga informasi yang ada pada berkas tersebut tidak dapat diketahui oleh pihak lain yang tidak berkepentingan.

Corresponding Author :
Nama : Herman Efendi
Kantor : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : hermanefendi139@gmail.com

1. PENDAHULUAN

Data laba penjualan merupakan data yang menyimpan arsip tentang laba bersih (*net profit*) yang telah dikurangi biaya-biaya yang menjadi beban perusahaan dalam suatu periode tertentu termasuk pajak. Laba bersih adalah keuntungan yang diperoleh oleh perusahaan setelah dikurangi dengan pajak penghasilan. Laba bersih dihitung sebagai hasil pengurangan antara laba sebelum pajak dengan beban pajak penghasilan [2].

PT. Efata Indonesia Tour & Travel ini adalah perusahaan yang bergerak dibidang penyedia layanan travel atau pariwisata. Penjualan dan laba pada perusahaan PT. Efata Indonesia Tour & Travel merupakan suatu hal yang sifatnya internal dan tidak semua pihak boleh mengetahuinya, termasuk kepada karyawan, terkecuali pada karyawan bagaian keuangan. Seiring dengan tuntutan akan keamanan untuk kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat, menimbulkan tuntutan tersedianya suatu sistem pengamanan data dan informasi yang lebih baik agar dapat mengamankan data dari berbagai ancaman.

Dari permasalahan yang telah dijelaskan diatas, diharapkan dapat dibangun sistem yang membantu PT. Efata Indonesia Tour & Travel dalam mengamankan data laba penjualan. Berdasarkan permasalahan tersebut, maka diangkatlah judul karya ilmiah yaitu **"Implementasi Kriptografi dalam Pengamanan Data Laba Penjualan pada PT. Efata Indonesia Tour & Travel dengan Metode Merkle Hellman".**

2. KAJIAN PUSTAKA

2.1 Pengertian Kriptografi

Kriptografi adalah ilmu teknik enkripsi dimana "naskah asli" (plaintext) diacak dengan menggunakan suatu kunci enkripsi menjadi "naskah acak yang akan susah dibaca" (*ciphertext*). Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata "Kriptografi" di bagi menjadi dua, yaitu Kripto dan Graphia. Dimana kripto yang memiliki arti secret (rahasia) dan Graphia berarti *writing* (tulisan) [7].

2.2 Algoritma Marke Hellman

Metode Merkle Hellman Merupakan salah satu sistem kripto yang mengunakan tipe kunci asimetri. Pada sistem merkle hellman ini, kunci yang digunakan adalah 2 kunci yang berbeda. Satu kunci untuk mengenkripsi dan satu kunci untuk mendekripsi [10].

2.3 Proses Enkripsi

Pada saat proses enkripsi, metode Merkle Hellman menggunakan rumus sebagai berikut :

$C = \Sigma^{n}_{i=1} \alpha i \beta_i$……..[2.1]

Keterangan :

α = Pesan / *Plaintext* β = *Public Key*

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

1. Membuat *Private Key*
   bulat yang disusun dengan algoritma *superincreasing linear, w* terdiri dari beberapa angka tergantung dari jumlah digit binner yang digunakan. q adalah nilai (angka) bebas yang harus lebih besar dari jumlah keseluruhan nilai *w*. Sedangkan r adalah nilai (angka) bebas yang dapat diambil mulai dari angka 1 sampai nilai q.
   Membuat urutan $w = (^{w}1, ^{w}2, \ldots, ^{w}n)$
   $q > \Sigma^{n}_{i=1} w_i$ . . . . . .[2.2]
2. Membuat *Public Key*
   Public key digunakan untuk menghitung hasil *chipper* data. *Public key* memiliki karakter yang sama dengan *private key*. Jika *private key* di lambangkan dengan w, maka *public key* dapat dilambangkan dengan β karena itu *public key* memiliki deretan angka sebagai kunci untuk mencari *chipper.*
   $\beta = w * r \bmod q$ ……[2.3]
3. Merubah Plainteks Ke Binner 8 Digit
   Pada proses ini data perlu diubah menjadi bentuk binner karena perhitungan Merkle Hellman menggunakan tehnik *binary* sebagai proses enkripsi dan dekripsinya. Untuk mengubah data ke *binery* 8 digit, maka sebelumnya data dirubah ke kode ASCII.
4. Menjumlahkan (Perkalian Binner Dengan *Public Key*)
   Untuk proses perhitungan data *chippertext,* terlebih dahulu harus melakukan pembagian *plaintext* ke dalam blok-blok berdasarkan jumlah elemen β. Diketahui jumlah elemen β sebanyak 8 elemen. Selanjutnya, setiap blok akan dikaitkan dengan setiap elemen β, sehingga diperoleh *chippertext.*
   $C = \Sigma^{nj}_{=1} \alpha j \beta j$ . . . . .[2.4]

2.4 Proses Dekripsi

Pada saat proses dekripsi, metode *Merkle Hellman* menggunakan model sebagai berikut :

$C = \Sigma^{n}_{1=1} X_1 W_1$ . . . . .[2.5]

Keterangan : W = *Private Key* X = Pesan / *Chippertex*

Adapun langkah-langkah dalam proses dekripsi dengan menggunakan metode Merkle Hellman adalah sebagai berikut

1. Data *Chippertext*
   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.
2. Modular *Invers*
   Proses untuk mencari nilai *modulo invers* dari (r^{-1}) dengan menggunakan
   metode *extended eucledian.* Dalam proses dekripsi ini akan digunakan nilai r^{-1}. Nilai M diperoleh dari hasil perhitungan menggunakan metode *extended eucledian*
   $M = (r * M \bmod p = 1)$. . . . . [2.6]
3. *Chipper* Data Mod q
   Proses berikutnya adalah proses mod, yaitu untuk data *chippertext* dengan nilai *invers* yang diperoleh sebelumnya.
   $K = C.r\text{-}1 \bmod q$ . . . . . [2.7]
4. Mengurangkan Data Dengan Nilai w

Proses pengurangan data (k) dengan nilai-nilai pada elemen w. Pengurangan terus dilakukan dari elemen yang paling besar hingga yang paling kecil. Hasil akhir dari pengurangan haruslah 0. Hasil akhir dimana pengurangan tidak nol, maka proses *dekripsi* dinyatakan gagal. Penyebab kegagalan dapat terjadi apabila kunci w tidak dibuat dengan metode *siperincreasing linier* [11]

3. METODE PENELITIAN

Metode Penelitian merupakan proses atau cara ilmiah untuk mendapatkan data yang akan digunakan untuk menyelesaikan masalah dengan dengan mengadakan studi langsung kelapangan untuk mengumpulkan data.
Adapun metode dalam penelitian ini mencakup :

1. Teknik Pengumpulan Data

Teknik pengumpulan data berupa suatu pernyataan tentang sifat, keadaan, kegiatan tertentu dan sejenisnya. Pengumpulan data dalam penelitian di PT. Efata Indonesia Tour & Travel menggunakan 4 cara berikut merupakan uraian yang digunakan :

a. Wawancara
   Pengumpulan data dengan melakukan tanya jawab langsung dengan narasumber dari objek yang diteliti untuk memperoleh yang diinginkan. Wawancara dilakukan guna mendapatkan alur kerja pada objek yang diteliti yang akan digunakan dalam menentukan fitur-fitur yang akan dibangun. Pada tahapan wawancara dilakukan dengan cara mewawancarai staff pada PT. Efata Indonesia Tour & Travel tentang data laba penjualan yang ingin diamankan.
b. Observasi
   Metode pengumpulan data ini digunakan untuk mendapatkan data yang berkaitan dengan peninjauan langsung ke PT. Efata Indonesia Tour & Travel dan melihat arsip yang dimiliki di kantor mereka.

2. Studi Kepustakaan (*Library Research*)
   Studi Kepustakaan merupakan salah satu elemen yang mendukung sebagai landasan teoritis peneliti untuk mengkaji masalah yang dibahas. Dalam hal ini, peneliti menggunakan beberapa sumber kepustakaan diantaranya: Buku, Jurnal Nasional, Jurnal Internasional dan Sumber-sumber lainnya yang berkaitan dengan Bidang ilmu Kriptografi

3.1 Metodologi Perancangan Sistem

Metode yang digunakan dalam perancangan ini menggunakan model proses atau paradigma *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*)

a. Analisis Masalah dan Kebutuhan
   Pada tahapan Analisis Masalah dan Kebutuhan, dilakukan dengan penelitian, wawancara ke PT. Efata Indonesia Tour & Travel . Dimana penelitian pada tahap ini dilakukan dengan cara mencari permasalahan dan persoalan persoalan tentang laba penjualan 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 dirancanglah tampilan program dan database yang akan digunakan pada sistem. Yang sebelumnya telah dimodelkan dengan menggunakan *Unified Modelling Language* (UML).
c. Pengkodean
   Pengkodean dilakukan dengan menterjemahkan hasil dari Perancangan dan Pemodelan ke dalam bahasa pemrograman berbasis *Desktop Programing* agar dikenali oleh komputer agar menjadi suatu sistem yang menjadi solusi dari permasalahan untuk mengamankan data laba penjualan 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 di ujicoba sendiri, dan melihat setiap detil program apakah berjalan sesuai dengan yang telah dirancang ataukah 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. Efata Indonesia Tour & Travel .
f. Implementasi Sistem

Implementasi merupakan tahapan akhir setelah sistem melalui 5 tahapan sebelumnya dan layak untuk digunakan. Pada tahapan ini dilihat pula perkembangan aplikasi, dan melihat sejauhmana aplikasi atau sistem dapat bekerja melakukan mengamankan data laba penjualan dengan akurat.

3.2 PENERAPAN METODE MERKLE HELLMAN

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

3.2.1 Membuat *Privat key* (S, A dan P)

S = (2,4,7,14,28,112,224,407) = ∑s = 798
A = 989
P = 578

3.2.2 Membuat *Public Key*

Plaintext (x) : TIKETPELNI
Enkripsi :
Perhitungan *Public Key*(T) :
T = P * Si mod A
T1 = 578 * 2 mod 989 = 167
T2 = 578 * 4 mod 989 = 334
T3 = 578 * 7 mod 989 = 90
T4 = 578 * 14 mod 989 = 180
T5 = 578 * 28 mod 989 = 360
T6 = 578 * 112 mod 989 = 451
T7 = 578 * 224 mod 989 = 902
T8 = 578 * 407 mod 989 = 853
Didapatkan
T = (167,334,90,180,360,451,902,853)

3.2.3 Mengubah Plaintext ke Biner Enkripsi

Pada Proses ini data perlu diubah menjadi bentuk biner karena perhitungan Merkle Hellman menggunakan teknik binary sebagai proses enkripsi dan dekripsinya
Plaintext :
TIKETPELNI
Dimasukkan kedalam kode ASCII
X = 84 73 75 69 84 80 69 76 78 73
Masing-masing kode ASCII kemudian di konversi ke binner.

Plaintext	ASCII	Binary(Z)
T	84	01010100
I	73	01001001
K	75	01001011
E	69	01000101
T	84	01010100
P	80	01010000
E	69	01000101
L	76	01001100
N	78	01001110
I	73	01001001

3.2.4 Menjumlahkan (perkalian *biner* dengan *Publik key*).

Plaintext dibagi dalam blok sesuai dengan banyaknyaS, pada contoh ini banyaknya S adalah 8 digit
01010100 : Y = (0*167) + (1*334) + (0*90) + (1*180) + (0*360) + (1*451) + (0*902) + (0*853) = 965
01001001 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (1*360) + (0*451) + (0*902) + (1*853) = 1547
01001011 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (1*360) + (0*451) + (1*902) + (1*853) = 2449
01000101 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (0*360) + (1*451) + (0*902) + (1*853) = 1638
01010100 : Y = (0*167) + (1*334) + (0*90) + (1*180) + (0*360) + (1*451) + (0*902) + (0*853) = 965
01010000 : Y = (0*167) + (1*334) + (0*90) + (1*180) + (0*360) + (0*451) + (0*902) + (0*853) = 514

01000101 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (0*360) + (1*451) + (0*902) + (1*853) = 1638
01001100 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (1*360) + (1*451) + (0*902) + (0*853) = 1145
01001110 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (1*360) + (1*451) + (1*902) + (0*853) = 2047
01001001 : Y = (0*167) + (1*334) + (0*90) + (0*180) + (1*360) + (0*451) + (0*902) + (1*853) = 1547
Ciphertext:

1547 2449 1638 965 514 1638 1145 2047 1547

3.2.5 Mengubah *Chipertext* ke *Plaintext* (*Dekripsi)*

Dekripsi :
Hitung $Z = M^{-1}Y \bmod A$
M^{-1} = ?????

M	P*M mod A	
1	578 * 1 mod 989	578
2	578 * 2 mod 989	167
3	578 * 3 mod 989	745
.....	…..* ... mod ……	.....
77	578 * 77 mod 989	1

M^{-1}= 77
$Z = M^{-1} * Y \bmod A$
Untuk Y ⟶ 965:
Z = 77 *965 mod 989 = 130
Untuk Y ⟶ 1547:
Z = 77 * 1547 mod 989 = 439
Untuk Y ⟶ 2449:
Z = 77 * 2449 mod 989 = 663
Untuk Y ⟶ 1638:
Z = 77 * 1638 mod 989 = 523
Untuk Y ⟶ 965:
Z = 77 * 965 mod 989 = 130
Untuk Y ⟶ 514 :
Z = 77 * 514 mod 989 = 18
Untuk Y ⟶ 1638 :
Z = 77 * 1638 mod 989 = 523
Untuk Y ⟶ 1145:
Z = 77 * 1145 mod 989 = 144
Untuk Y ⟶ 2047:
Z = 77 * 2047 mod 989 = 368
Untuk Y ⟶ 1547 :
Z = 77 * 1547 mod 989 = 439

3.2.4 Mengurangkan Data Dengan Nilai S

Proses pengurangan data 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 0, maka proses dekripsi dinyatakan gagal. Penyebab kegagalan dapat terjadi apabila kunci S tidak dibuat dengan metode *superincreasing linier*.

Untuk Y ⟶ 965 = 130

2	4	7	14	28	112	224	407	S
							130-407	Z
						130 -224		
					130 -112			
				18 - 28	18			

			18- 14					
		4-7	4					
	4-4							
0-2								
0	1	0	1	0	1	0	0	

Plaintext : 01010100

Untuk Y ⟶ 1547 = 439

2	4	7	14	28	112	224	407	S
							439 - 407	Z
						32 -224	32	
					32-112			
				32-28				
			4-14	4				
		4–7						
	4-4							
0 - 2	0							
0	1	0	0	1	0	0	1	

Plaintext : 01001001

Untuk Y ⟶ 2449 = 663

2	4	7	14	28	112	224	407	S
							663 - 407	Z
						256-224	256	
					32-112	32		
				32-28				
			4-14	4				
		4–7						
	4-4							
0 - 2	0							
0	1	0	0	1	0	1	1	

Plaintext : 01001011

Untuk Y ⟶ 1638= 523

2	4	7	14	28	112	224	407	S
							523 - 407	Z
						116 -224	116	
					116-112			
				4-28	4			
			4-14					

		4–7						
	4-4							
0 - 2	0							
0	1	0	0	0	1	0	1	

Plaintext : 01000101

Untuk Y ⟶ 965 = 130

2	4	7	14	28	112	224	407	S
							130 - 407	Z
						130-224		
					130-112			
				18-28	18			
			18-14					
		4–7	4					
	4-4							
0 - 2	0							
0	1	0	1	0	1	0	0	

Plaintext : 01010100

Untuk Y ⟶ 514 = 18

2	4	7	14	28	112	224	407	S
							18 - 407	Z
						18 -224		
					18-112			
				18 -28				
			18-14					
		4-7	4					
	4-4							
0-2	0							
0	1	0	1	0	0	0	0	

Plaintext : 01010000

Untuk Y ⟶ 1638 = 523

2	4	7	14	28	112	224	407	S
							523 - 407	Z
						116 - 224	116	
					116-112			
				4 -28	4			
			4 -14					

		4 -7						
	4-4							
0-2	0							
0	1	0	0	0	1	0	1	

Plaintext : 01000101

Untuk Y ⟶ 1145= 144

2	4	7	14	28	112	224	407	S
							144 - 407	Z
						144 -224		
					144-112			
				32-28	32			
			4-14	4				
		4–7						
	4-4							
0 - 2	0							
0	1	0	0	1	1	0	0	

Plaintext : 01001100

Untuk Y ⟶ 2047= 368

2	4	7	14	28	112	224	407	S
							368-407	Z
						368-224		
					144-112	144		
				32-28	32			
			4-14	4				
		4-7						
	4-4							
0-2	0							
0	1	0	0	1	1	1	0	

Plaintext : 01001110

Untuk Y ⟶ 1547= 439

2	4	7	14	28	112	224	407	S
							439-407	Z
						32-224	32	
					32 -112			
				32 - 28				
			4- 14	4				

		4-7						
	4-4							
0-2								
0	1	0	0	1	0	0	1	

Plaintext : 01001001

Plaintext dimasukan ke dalam kode ASCII maka akan didapatkan hasil

Binary(Z)	ASCII	Plaintext
01010100	84	T
01001001	73	I
01001011	75	K
01000101	69	E
01010100	84	T
10010000	80	P
01000101	69	E
01001100	76	L
01001110	78	N
01001001	73	I

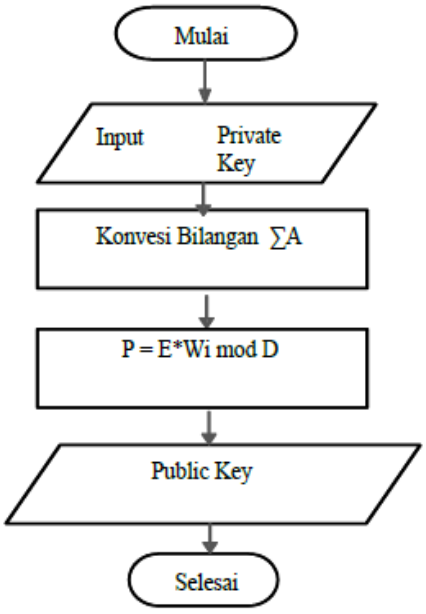
Maka akan menjadi : TIKETPELNI

3.3 Algoritma Sistem

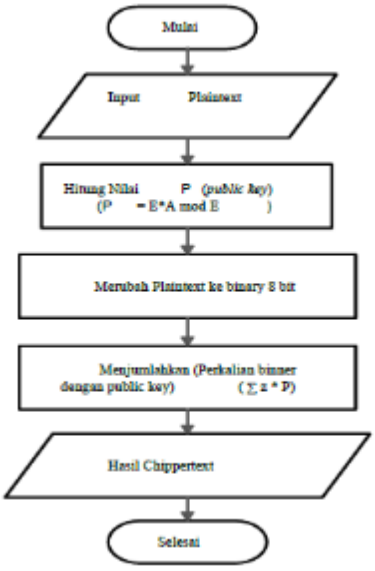
Algoritma Sistem merupakan langkah-langkah yang dilakukan sebuah sistem dalam memproses dan menyelesaikan suatu permasalahan. Berikut ini adalah flowchart atau alur dari pemecahan permasalahan dengan menggunakan metode Merkle Hellman.

3.3.1 Pembentukan Kunci, Enkripsi Dan Dekripsi

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



Gambar 3.1 Flowchat Kunci



Gambar 3.2 Flowchat Enkripsi

Gambar 3.3 Flowchat Dekripsi

3.4 ANALISA DATA DAN HASIL

3.4.1 Implementasi

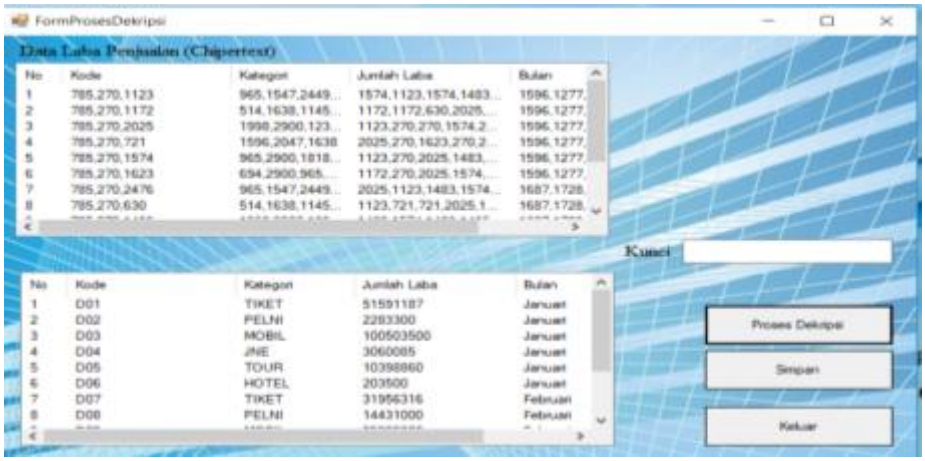
Implementasi system adalah tahapan dimana sistem atau aplikasi siap untuk dioperasikan pada keadaan yang sebenarnya sesuai dari hasil analisis dan perancangan yang dilakukan, sehingga akan diketahui apakah sistem atau aplikasi yang dirancang benar-benar dapat menghasilkan tujuan yang dicapai.

1. *Form* Proses Enkripsi

Berikut adalah tampilan *form* Proses Enkripsi:

2. *Form* Proses Dekripsi

Berikut adalah tampilan *form* Proses Dekripsi:



3.5 KELEMAHAN DAN KELEBIHAN SISTEM

Adapun kelemahan dari sistem ini adalah sebagai berikut:

1. Aplikasi ini hanya mampu menyamarkan data laba penjualan dan menyimpannya kedalam *database*, apabila *database* diacak tentu akan sulit untuk mendekripsikannya kembali
2. Metode *merkle hellman* memiliki kunci yang tidak sembarang dan hanya bisa diisi oleh bilangan yang co-prima, itu artinya untuk memberikan kunci pada plaintext tidak bisa menggunakan karakter huruf.
3. Hasil enkripsi *merkle hellman* berupa angka dengan susunan acak, bukan berupa bilangan acak dengan makna ASCII.

Adapun Kelebihan sistem ini adalah sebagai berikut:

1. Aplikasi ini mampu melakukan pengamanan data yang cukup kuat.
2. Aplikasi ini mampu digunakan dalam mengamankan data laba penjualan.
3. Sistem ini dipermudah dengan nilai kunci yang *default* meskipun *user* tidak menginputkan kuncinya, sistem akan menerapkan kunci *default* yang hanya diketahui oleh *user*.

4 KESIMPULAN DAN SARAN

4.1 KESIMPULAN

Berdasarkan analisa pada permasalahan yang terjadi dalam kasus yang diangkat tentang mengamankan data laba penjualan PT. Efata Indonesia Tour & Travel, maka dapat ditarik kesimpulan sebagai berikut:

1. Berdasarkan hasil penelitian yang telah dilakukan sebelumnya, dalam menganalisis permasalahan terkait dalam mengamankan data laba penjualan dengan menggunakan Ilmu Kriptografi menggunakan metode *Merkle Hellman* dilakukan dengan cara mencari tahu kebutuhan PT. Efata Indonesia Tour & Travel dalam mengamankan data laba penjualan.
2. Dalam menerapkan metode *Merkle Hellman* dalam mengamankan data laba penjualan diterapkan dengan cara mengolah data laba penjualan kemudian mencoba mengenkripsikan dan mendekripsikan data tersebut dengan metode *Merkle Hellman*.
3. Dalam merancang dan membangun aplikasi pengamanan data laba penjualan dapat menggunakan bantuan pemodelan UML terlebih dahulu, dengan kata lain aplikasi digambarkan pada bentuk *Use Case Diagram, Activity Diagram* dan *Class Diagram.* Kemudian dilakukan pengkodean dengan perancangan tersebut.
4. Dalam menguji aplikasi pengamanan data laba penjualan dilakukanlah penerapan aplikasi tersebut di PT. Efata Indonesia Tour & Travel, setelah itu melihat seberapa cocok kinerja aplikasi tersebut dengan yang dibutuhkan pihak perusahaan

4.2 SARAN

Untuk meningkatkan kemampuan dan fungsi dari program ini ada beberapa saran yang dapat diberikan untuk pengembangan yang bisa dilakukan yaitu:

1. Program yang dibuat ini masih dapat dikembangkan lebih lanjut supaya menjadi sistem yang lebih lengkap berdasarkan dengan kepentingan yang lebih luas.
2. Aplikasi ini dapat menggunakan metode lain seperti *RC4, AES, RSA* dan lainnya, agar kunci dari enkripsi aplikasi tersebut dapat diubah secara dinamis dengan menggunakan karakter huruf.

DAFTAR PUSTAKA

[2] Denny Putri Hapsari, "ANALISIS PENJUALAN BERSIH, BEBAN UMUM & ADMINISTRASI TERHADAP LABA TAHUN BERJALAN," *Jurnal Akuntansi*, vol. 5, no. 1, 2018.

[7] M. E. A. Ely Setyo Astuti, Binar Prihadmantyo, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI MERKLE HELLMAN DAN METODE," *Jurnal Teknologi Informatika dan Terapan* , vol. 4, no. 2, pp. 81-87, 2017.

[10] DediLeman, "METODE MERKLE HELLMAN UNTUK ENKRIPSI DAN DEKRIPSI PESAN WHATAPP," *RiauJournalofComputerScience*, vol. 6, no. 1, 2020.

[11] L. Purba and G. Leonarde Ginting, "Aplikasi Enkripsi dan Dekripsi Teks Menggunakan Algoritma Merkle Hellman," *MEANS (Media Informasi Analisa dan Sistem)*, vol. 4, no. 1, 2019.

BIBLIOGRAFI PENULIS

	**Data Diri** Nama : Herman Efendi Tempat/Tanggal lahir : Pematang Ibul, 09 Maret 1997 Jenis Kelamin : Laki-laki Agama : Kristen Protestan Kewarganegaraan : Indonesia Alamat : Jln. Bunga Cempaka, Gang Famili No. 01, Medan Email : hermanefendi139@gmail.com **Latar Belakang Pendidikan** 2003 – 2009 : SD NEGERI 007 Pematang Ibul 2009 – 2012 : SMP Negeri 3 Bangko Pusako 2012 – 2015 : SMK Swasta GKPS 2 Pematang Siantar 2016 – 2020 : STMIK Triguna Dharma
	Faizal Taufik, S.Kom., M.Kom
	Devri Suherdi, S.Kom., M.Kom