Jurnal Cyber Tech
Vol.x, No.x, Juli 2020, pp. xx~xx
P-ISSN :
E-ISSN :

KEAMANAN DATA PENJUALAN BULANAN PADA UNIT USAHA PUSAT KOPERASI KARTIKA "A" BUKIT BARISAN DENGAN ALGORITMA MERKLE HELLMAN

Romauli Simanullang *, Badrul Anwar **, Ismawardi Santoso **
* Program StudiSistemInformasi, STMIK Triguna Dharma
** Program StudiSistemInformasi, STMIK Triguna Dharma

Article Info
Article History:
-

Keyword:
Kriptografi, Merkle Hellman, Data Penjualan, Desktop

ABSTRACT

Data penjualan bulanan adalah sekumpulan data penjualan yang disusun dan di informasikan sebagai bahan pencatatan dan analisa penjualan. Data penjuaalan sendiri memiliki fungsi dan harus benar-benar akurat tanpa adanya kesalahan. Setiap laporan yang dibuat tentu secara tidak langsung bertindak sebagai media untuk menyampaikan informasi tentang perubahan yang ada dalam penjualan apakah itu kenaikan atau penurunan, mengirimkan informasi data penjualan terperinci juga membuat penerima informasi atau data lebih cepat memahami konidisi data penjualan bulanan. Tujuan dari skripsi ini adalah untuk mengamankan data penjualan. Ada cara untuk mengamankan data penjualan agar data tersebut tetap aman dan tidak diubah oleh pihak lain, yaitu dengan menggunakan KriptografiKriptografi merupakan seni dan ilmu untuk menjaga keamanan data dengan mengubahnya menjadi kode tertentu, dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali, yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dan untuk penerapan kriptografi terdapat beberapa metode atau algoritma, salah satunya adalah Merkle Hellman

Corresponding Author :
Nama : Romauli Simanullang
Kantor : STMIK Triguna Dharma
Program Studi : SistemInformasi
E-Mail : romamanullang27@gmail.com

1. PENDAHULUAN

Pada kemajuan era globalisasi dengan pesatnya perkembangan ilmu teknologi informasi dan teknologi saat ini, dikala teknologi menjadi asupan sehari-hari masyarakat, mengakibatkan setiap orang dengan mudahnya mengirim dan menerima sebuah data. Keamanan data adalah suatu hal yang sangat penting agar ancaman pada proses pertukaran data terjaga dan dapat diproses, terutama dokumen maupun data yang diasumsikan bersifat rahasia. Seperti yang diketahui dimana pertukaran data sangatlah penting dan bisa menguntungkan kepada beberapa organisasi, perguruan tinggi, individual, dan lembaga pemerintah [1]. Kriptografi sendiri merupakan salah satu teknik penyandian untuk menjaga keamanan data yang digunakan untuk mengamankan data dari pertukaran suatu informasi[3]. Dalam kriptografi ada beberapa algoritma yang dapat digunakan untuk melakukan enkripsi dan dekripsi, salah satu nya adalah algoritma Merkle Hellman[4].

2. KAJIAN PUSTAKA

2.1 Pengertian Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa Yunani yaitu *cryptos* yang artinya "*secret*"(yang tersembunyi) dan *graphein* yang artinya "*writting*"*(*tulisan). Jadi Kriptografi berarti "secret writting"(tulisan rahasia).[5] Kriptografi adalah sebuah teknik rahasia dalam penulisan, dengan menggunakan karakter khusus, dan menggunakan huruf dan karakter di luar bentuk aslinya ataupun dengan metode-metode yang lain yang hanya bisa dipahami pihak-pihak yang memproses kunci. Kriptografi merupakan sebuah studi teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, otentikasi entitas serta otentikasi keaslian data dan integritas data. Kriptografi tidak hanya penyediaan keamanan informasi saja, tetapi juga sebuah himpunan teknik-teknik.[6]

2.2 *Merkle Hellman*

Merkle-Hellman Knapsack merupakan kripto sistem yang menggunakan algoritma asimetris dan memiliki 2 kunci utama, yakni kunci publik dan kunci privat. Kelebihan algoritma asimetris ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasian. Karena kunci yang didistribusikan adalah kunci publik. Sehingga jika kunci ini sampai hilang atau diketahui oleh orang lain yang tidak berhak, maka pesan sandi yang dikirim akan tetap aman. Sedangkan kunci private tetap disimpan (tidak didistribusikan). Kelebihan lain adalah pada efisiensi jumlah kunci publik. Jika terdapat n user, maka hanya membutuhkan 1 (satu) kunci publik, sehingga untuk jumlah user yang sangat banyak, sistem ini sangat efisien.

2.2.1 Proses Enkripsi

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

1. Membuat *private Key* (W, Q, R)
   Nilai W, Q, R adalah bilangan bulat yang disusun dengan algoritma *superincreasing linear*. S terdiri dari beberapa angka tergantung dari jumlah digit biner yang digunakan. A adalah nilai (angka) bebas yang harus lebih besar dari jumlah keseluruhan nilai S. Sedangkan P adalah nilai (angka) bebas yang dapat diambil mulai dari angka 1 sampai nilai Q.
   Membuat urutan s =($^{s}1$, $^{s}2$,....,^{s}n)
   q > $\sum^{n}$i=1 Wi……2.1
2. Membuat *Public Key*
   Public Key digunakan untuk menghitung hasil *chipper* data. *Public Key* memiliki karakter yang sama dengan *private key*. Jika *private key* dilambangkan dengan S, maka *public key* dapat dilambangkan dengan T karena itu *public key* memiliki deretan angka sebagai kunci untuk mencari *chipper*.
   β= W * Ri *mod Q*.... 2.2
3. Merubah Plainteks ke Biner 8 Digit
   Pada proses ini data perlu diubah menjadi bentuk biner 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 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.*
   C = $\sum^{z}$ * β….2.3

2.2.2 Proses Dekripsi

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

1. Data *Chippertext* (C)
   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* (M)
   Proses untuk mencari nilai *modulo invers* dari (p-¹) dengan menggunakan metode *extended eucledian*. Dalam proses dekripsi ini akan digunakan nilai p-¹. Nilai M diperoleh dari hasil perhitungan menggunakan metode *extended eucledian.*
   M = (R * M mod Q = 1)……..2.4
3. *Chipper* Data Mod Q
   Proses berikutnya adalah proses mod, yaitu untuk data *chippertext* dengan nilai *invers* yang diperoleh sebelumnya.
   K = (C * M) mod Q....2.5
4. Mengurangkan Data Dengan Nilai W
   Proses pengurangan data (K) dengan nilai-nilai pada elemen S. Pengurangan terus dilakukan darri 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 S tidak dibuat dengan metode *siperincreasing linier.*

3. METODOLOGI PENELITIAN

3.1 Metode Penelitian

Berikut metode penelitian yang digunakan dalam penelitian ini adalah:

1. 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, dan sumber lainnya.
2. Observasi

Observasi merupakan teknik pengumpulan data dengan melakukan tinjauan langsung ketempat studi kasus dimana akan dilakukan penelitian. Dalam hal ini peneliti melakukan observasi di Pusat Koperasi Kartika "A" Bukit Barisan.

3. Wawancara
   Teknik wawancara ini dilakukan untuk mendapatkan informasi tambahan dari pihak-pihak yang memiliki wewenang dan berinteraksi langsung dengan sistem yang akan dirancang sebagai sumber data.

3.3.2 Proses Enkripsi

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

1. Membuat Private Key (W, Q, R)

Tabel 3.2 *Private Key*

W	{ 2, 4, 7, 14, 28, 57, 115, 230 }=Σ^s = 457
Q	611
R	31

2. Membuat *Public Key*

Tabel 3.2 *Public Key*

W	P= (R * Wi) mod Q	
2	31 * 2 mod 611	62
4	31 * 4 mod 611	124
7	31 * 7 mod 611	217
14	31 * 14 mod 611	434
28	31 * 28 mod 611	257
57	31 * 57 mod 611	545
115	31 * 115 mod 611	510
230	31 * 230 mod 611	409

Maka Hasil proses *Public Key* adalah: P { 62, 124, 217, 434, 257, 545, 510, 409 }

3. Merubah *Plaintext* ke Binner 8 Digit
   Plaintext: PUSKOPKAR "A"

Tabel 3.2 Data *Binnary*

Plaintext	**ASCII**	**Binnary**
P	80	01010000
U	85	01010101
S	83	01010011
K	75	01001011
O	79	01001111
P	80	01010000
K	75	01001011
A	73	01000001
R	82	01010010
Space	32	00100000
„	34	00100010
A	65	01000001
„	34	00100010

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

Tabel 3.2 Proses Perhitungan Data *Chippertext*

Binary (z)	**∑z * P**	**Chippertext**
01010000	(0*62)+(1*124)+(0*217)+(1*434)+ (0*257)+(0*545)+(0*510)+(0*409)	558
01010101	(0*62)+(1*124)+(0*217)+(1*434)+ (0*257)+(1*545)+(0*510)+(1*409)	1512
	(0*62)+(1*124)+(0*217)+(1*434)+	

01010011	(0*257)+(0*545)+(1*510)+(1*409)	1477
01001011	(0*62)+(1*124)+(0*217)+(0*434)+ (1*257)+(0*545)+(1*510)+(1*409)	1300
01001111	(0*62)+(1*124)+(0*217)+(0*434)+ (1*257)+(1*545)+(1*510)+(1*409)	1845
01010000	(0*62)+(1*124)+(0*217)+(1*434)+ (0*257)+(0*545)+(0*510)+(0*409)	558
01001011	(0*62)+(1*124)+(0*217)+(0*434)+ (1*257)+(0*545)+(1*510)+(1*409)	1300
01000001	(0*62)+(1*124)+(0*217)+(0*434)+ (0*257)+(0*545)+(0*510)+(1*409)	533
01010010	(0*62)+(1*124)+(0*217)+(1*434)+ (0*257)+(0*545)+(1*510)+(0*409)	1068
00100010	(0*62)+(0*124)+(1*217)+(0*434)+ (0*257)+(0*545)+(0*510)+(0*409)	217
00100010	(0*62)+(0*124)+(1*217)+(0*434)+ (0*257)+(0*545)+(1*510)+(0*409)	727
01000001	(0*62)+(1*124)+(0*217)+(0*434)+ (0*257)+(0*545)+(0*510)+(1*409)	533
00100010	(0*62)+(0*124)+(1*217)+(1*434)+ (0*257)+(0*545)+(1*510)+(0*409)	727

C = {558, 1512, 1477, 1300, 1845, 558, 1300, 533, 1068, 217, 727, 533, 727,}

3.3.3 Proses Dekripsi

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

1. Data Chippertext (C)
   Dalam melakukan proses dekripsi, terlebih dahulu harus ada data yang lengkap dari proses enkripsi, selain itu *private key* juga dibutuhkan sebagai kunci untuk proses dekripsi data.
   Kode *chippertext* adalah sebagai berikut:
   C = {558, 1512, 1477, 1300, 1845, 558, 1300, 533, 1068, 217, 727, 533, 727,}
2. Modular Invers(M)
   Proses untuk mencari nilai modulo invers dari (p^{-1}) dengan menggunakan metode *extended eucledian*, yaitu (R * M mod Q= 1). Dalam proses dekripsi ini akan digunakan nilai (p^{-1}). Nilai (p^{-1}) diperoleh dari hasil perhitungan menggunakan metode *extended eucledian*, seperti table dibawah ini:

Tabel 3.3 Proses Perhitungan M Invers

M	**(R * M) mod Q**	
1	31 * 1 mod 611	31
2	31 * 2 mod 611	62
3	31 * 3 mod 611	93
....	….	….
138	31 * 138 mod 611	1

3. Chipper Data Mod Q

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

Tabel 3.3 Chipper Data Mod Q

Chipper (C)	**M**	**K = (C * M) mod Q**	
558	138	558 * 138 mod 661	18
1512	138	1512 * 138 mod 661	305
1477	138	1477 * 138 mod 661	363
1300	138	1300 * 138 mod 661	377
1845	138	1845 * 138 mod 661	434
558	138	558 * 138 mod 661	18
1300	138	1300 * 138 mod 661	377
533	138	533 * 138 mod 661	234
1068	138	1068 * 138 mod 661	133
217	138	217 * 138 mod 661	7
727	138	727 * 138 mod 661	122
533	138	533 * 138 mod 661	234
727	138	727 * 138 mod 661	122

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 bernilai 0. Hasil akhir dimana pengurangan tidak nol, maka proses dekripsi dinyatakan gagal. Penyebab kegagalan dapat terjadi apabila kunci W tidak dibuat dengan metode *superincreasing linier*.

W = {2,4,7,14,28,57,115,230}

K = {18,305,363,377,434,18,377,234,,133,7,122,234,122}

Tabel 3.3 Proses Pengurangan *Chippertext*

2	4	7	14	28	57	115	230	**W**
							18-230	**K**
						18-115		
					18-57			
				18-28				
			18-14					
			4					
		4-7						
	4-4							
	0							
0-2								
0	**1**	**0**	**1**	**0**	**0**	**0**	**0**	

Proses perhitungan pada table diatas dimulai dari kolom kanan lalu kekolom kiri, kolom K dikurangi dengan kolom W, jika kolom K dan kolom W dapat dikurangkan dan menghasilkan nilai positif maka akan menghasilkan bilangan binernya adalah *true* atau 1, jika kolom K dan kolom W saat dikurangkan mendapatkan hasil negative maka bilangan binernya adalah *false* atau 0, pada kolom selanjutnya hasil dari pengurangan kolom sebelumnya akan dikurangkan dengan bilangan W, lalu teruskan pengurangan pada setiap kolom. Apabila hasil data tersebut diambil keseluruhan maka akan menghasilkan nilai "01000001" yang apabila dikembangkan ke kode decimal menjadi "65" dan ke char menjadi "W". Proses berikutnya, nilai v1 sampai v18 akan dikomposisi menggunakan setiap nilai pada W. Dekomposisi ini dilakukan dengan cara pengurangan terhadap nilai tersebut sampai terkecil dan menghasilkan vi=0.

V1 = 18 – 230 (0)
= 18 – 115 (0)
= 18 – 57 (0)
= 18 – 28 (0)
= 18 – 14 (1)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01010000 = 80 (P)

V2 = 305 – 230 (1)
= 75 – 115 (0)
= 75 – 57 (1)
= 18 – 28 (0)
= 18 – 14 (1)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01010101 = 85 (U)

V3 = 363 – 230 (1)
= 133 – 115 (1)
= 18 – 57 (0)
= 18 – 28 (0)
= 18 – 14 (1)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01010011 = 83 (S)

V4 = 377 – 230 (1)
= 147 – 115 (1)
= 32 – 57 (0)
= 32 – 28 (1)
= 4 – 14 (0)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01001011 = 75 (K)

V5 = 434 – 230 (1)
= 204 – 115 (1)
= 89 – 57 (1)
= 32 – 28 (1)
= 4 – 14 (0)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01001111 = 79 (O)

V6 = 18 – 230 (0)
= 18 – 115 (0)
= 18 – 57 (0)
= 18 – 28 (0)
= 18 – 14 (1)
= 4 – 7 (0)
= 4 – 4 (1)

= 0 – 2 (0)
= 01010000 = 80 (P)
V7 = 377 – 230 (1)
= 147 – 115 (1)
= 32 – 57 (0)
= 32 – 28 (1)
= 4 – 14 (0)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01001011 = 75 (K)
V8 = 234 – 230 (1)
= 4 – 115 (0)
= 4 – 57 (0)
= 4 – 28 (0)
= 4 – 14 (1)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01000001 = 65 (A)
V9 = 122 – 230 (0)
= 122 – 115 (1)
= 7 – 57 (0)
= 7 – 28 (0)
= 7 – 14 (1)
= 7 – 7 (1)
= 0 – 4 (0)
= 0 – 2 (0)
= 00100010 = 82 (R)
V10 = 7 – 230 (0)
= 7 – 115 (0)
= 7 – 57 (0)
= 7 – 28 (0)
= 7 – 14 (0)
= 4 – 7 (1)
= 0 – 4 (0)
= 0 – 2 (0)
= 00100000 = 32 (Space)
V11 = 122 – 230 (0)
= 122 – 115 (1)
= 7 – 57 (0)
= 7 – 28 (0)
= 7 – 14 (0)
= 7 – 7 (1)
= 0 – 4 (0)
= 0 – 2 (0)
= 00100010 = 34 (“)
V12 = 234 – 230 (1)
= 4 – 115 (0)
= 4 – 57 (0)
= 4 – 28 (0)
= 4 – 14 (1)
= 4 – 7 (0)
= 4 – 4 (1)
= 0 – 2 (0)
= 01000001 = 65 (A)
V13 = 122 – 230 (0)
= 122 – 115 (1)
= 7 – 57 (0)
= 7 – 28 (0)
= 7 – 14 (0)

= 7 – 7 (1)
= 0 – 4 (0)
= 0 – 2 (0)
= 00100010 = 34 (“)

5. Mengembalikan ke Data Asli
   Mengembalikan ke data asli adalah hubungan tahapan terakhir untuk menkonversi enkripsi ke proses dekripsi. Adapun kode *binary* disusun dan dikonversikan ke kode decimal lalu ke kode char.
   C = {558,1512,1477,1300,1845,558,1300,533,1068,217,727,533,727}
   Z = {PUSKOPKAR “A”}

4. IMPLEMENTASI DAN PENGUJIAN

Implementasi merupakan tahap dimana 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. Aplikasi Sistem Pakar ini dilengkapi dengan *user interface* yang menarik dan bertujuan untuk memudahkan pengguna dalam menggunakannya. Pada aplikasi ini memiliki *interface* atau desain form yang terdiri dari form *Login*, form menu utama, form kerusakan, form gejala, form Basis Aturan, Form Deteksi, dan form laporan.

1. *Form Login*

Berikut ini merupakan tampilan dari *Form* Login yang berfungsi untuk melakukan proses validasi *username* dan *password pengguna:*

Gambar 5.1 *Form Login*

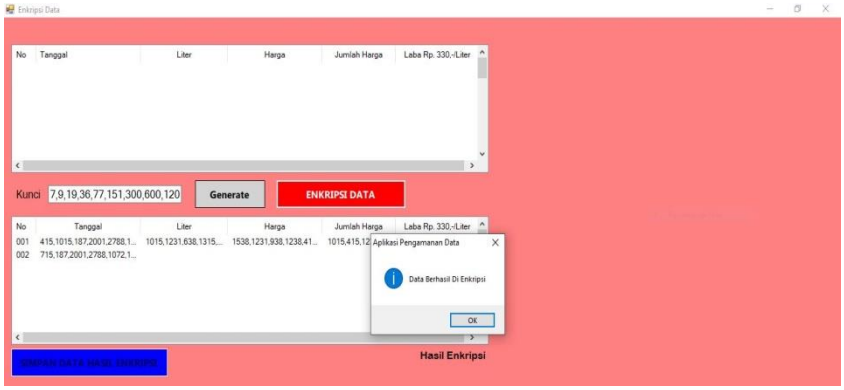
2. *Form* Menu Utama

Berikut ini merupakan tampilan menu utama dari pengamanan data nilai pada SMKS Teladan Sumatera Utara 2 menggunakan metode Merkle Hellman:

Gambar 5.2 *Form* Menu Utama

3. *Form* Enkripsi

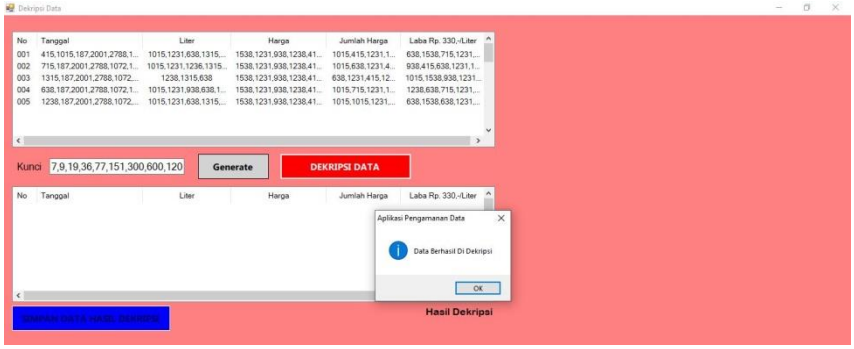
Berikut ini merupakan tampilan dari Form Enkripsi yang berfungsi untuk mengenkripsi data nilai pada SMKS Teladan Sumatera Utara 2:



Gambar 5.3 *Form* Enkripsi

4. *Form* Dekripsi

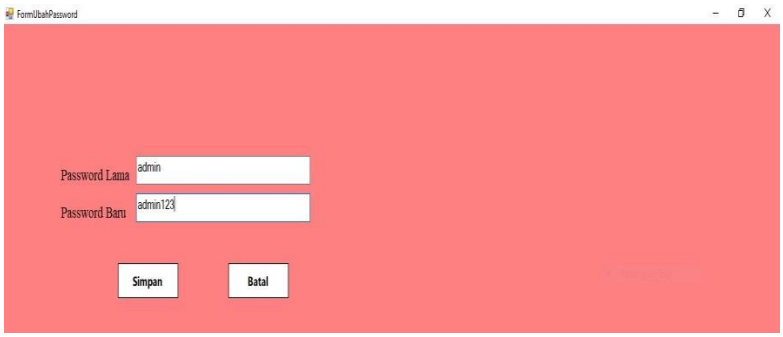
Berikut ini merupakan tampilan dari Form Dekripsi yang berfungsi untuk mendekripsi data nilai pada SMKS Teladan Sumatera Utara 2:



Gambar 5.4 *Form* Dekripsi

5. *Form* Ubah Password

Berikut ini merupakan tampilan dari *Form* Ubah Password yang berfungsi untuk melakukan proses ubah *password*



Gambar 5.5 *Form* Ubah Password

4 Kesimpulan

Berdasarkan uraian pembahasan analisa dan pengujian yang telah dilakukan, maka dapat diambil beberapa kesimpulan terhadap Keamanan data penjualan bulanan Pada unit Pusat Koperasi Kartika "A" Bukit Barisan dengan algoritma Merkle Hellman. Maka hasil pembahasan yang ada, ditarik beberapa kesimpulan:

1. Hasil dari analisis adalah dapat menerapkan metode Merkle Hellman untuk mengamankan data penjualan bulan pada unit usaha pusat koperasi kartika "A" Bukit barisan.
2. Metode Merkle Hellman dapat melindungi data dari orang yang tidak bertanggng jawab agar tidak disalah gunakan.
3. Berdasarkan Pengujian dari aplikasi yang dibuat berkenaan dengan penerapan kriptografi menggunakan metode merkle Hellman hasilnya adalah sinkron antara perangkat lunak dan perhitungan manual.

REFERENSI

[1] D. Juardi, "Pengamanan Data Dengan Penggabungan Metode Gost Dan Rc6," *Politek. Tri Mitra Karya Mandiri*, vol. 2, no. 2, pp. 1–9, 2013.

[3] K. Nisa, M. F. Rohmah, and Sugianto, "RANCANG BANGUN APLIKASI KRIPTOGRAFI DENGAN METODE ENKRIPSI FILE MENGGUNAKAN GABUNGAN ALGORITMA DES DAN CAESAR CHIPER UNTUK KEAMANAN DOKUMEN (Design," *Majapahit Techno*, vol. 6, no. 2, TEKS , ISI FILE DOKUMEN , DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION,"

vol. 10, no. 1, 2015.

[4] A. Aminudin, A. F. Helmi, and S. Arifianto, "Analisa Kombinasi Algoritma Merkle-Hellman Knapscak dan Logaritma Diskrit pada Aplikasi Chat," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 3, p. 325, 2018, doi: 10.25126/jtiik.201853844.

[5] M. Simanjuntak, "Implementasi Algoritma Merkle Hellman untuk Keamanan Database," *MEANS (Media Inf. Anal. dan Sist.*, vol. 4, no. 1, pp. 46–50, 2019.

[6] A. Moses, C. Satria, M. Gultom, R. I. Ndaumanu, T. Informatika, and W. Dharma, "Penerapan Metode Algoritma Gost Pada Perancangan Aplikasi Kriptografi," *J. InTekSis*, vol. 4, no. 2, p. 11, 2013.

BIOGRAFI PENULIS

	**Romauli Simanullang** Wanita kelahiran Doloksanggul, 27 November 1997 anak ke 6 dari 8 bersaudara pasangan Bapak Lanton Simanullang dan ibu Delima Situmorang, Mempunyai pendidikan Sekolah Dasar SD Inpres 174533 Matiti tamat tahun 209, kemudian melanjutkan pendidikan Sekolah Menengah Pertama SMP Swasta SRO Matiti 2012, kemudian melanjutkan pendidikan Sekolah Menengah Atas SMA Negeri 2 Doloksanggul tamat tahun 2015. Saat ini menempuh pendidikan Strata Satu (S-1) di STMIK Triguna Dharma Medan mengambil jurusan Program Studi Sistem Informasi. E-mail romamanullang27@gmail.com
	**Badrul Anwar, SE, S.Kom., M.Kom** Beliau merupakan dosen tetap STMIK Triguna Dharma, serta aktif sebagai dosen pengajar khusus pada bidang ilmu Sistem Informasi.
	**Ismawardi Santoso, S.Pd., MS** Beliau merupakan dosen tetap di STMIK Triguna Dharma serta aktif sebagai dosen pengajar khusus di bidang ilmu Sistem Informasi.