J-SISKO TECH
Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
P:ISSN : 2621-8976 E-ISSN : 2615-5133 ■ 56
Vol.4, No.1, Januari 2021, pp.56-68

IMPLEMENTASI KRIPTOGRAFI MERKLE HELLMAN DALAM MENGAMANKAN DATA NILAI SISWA SMK WIRA KESUMA JAYA KEC. NAMO RAMBE.

Purwadi
Program Studi Sistem Informasi, STMIK Triguna Dharma

ABSTRAK

Nilai adalah pencapaian hasil belajar peserta didik secara komulatif dalam satu semester. komulatif artinya perata-rataan dari rata-rata nilai ulangan harian, ulangan tengah semester, dan ulangan akhir semester. Data nilai siswa adalah suatu bentuk informasi penting yang diterima oleh siswa dari hasil proses belajar dan pembelajaran, baik itu nilai rapor, ijazah, nilai ulangan sehari hari dan sebagainya. Data nilai siswa juga digunakan untuk mengetahui sampai mana pemahaman siswa saat terjadinya proses pembelajaran . Hasil belajar siswa juga banyak dipengaruhi oleh beberapa faktor diantaranya faktor internal dan eksternal. Faktor internalnya yaitu faktor yang berasal dari dalam individu yang belajar, contoh jasmani dan rohani. Sedangkan faktor eksternalnya adalah faktor yang berasal dari luar individu itu sendiri, contoh keluarga, sekolah, dan masyarakat.

Pada permasalahan yang dibahas, dapat menerapkan Perancangan Aplikasi Keamanan Data salah satunya ialah menggunakan algoritma Markle Hellman dalam mengamankan data nilai siswa. Dengan mengamankan data nilai siswa bertujuan untuk membantu PKS Kurikulum dalam mengamankan data nilai siswanya.

Hasil penelitian merupakan terciptanya sebuah aplikasi Pengamanan Data dengan Algoritma Markle Hellman yang dapat membantu PKS Kurikulum dalam mengamankan data nilai siswa.

Kata Kunci *: Kriptografi, Markle Hellman, dan Data Nilai Siswa*

ABSTRACT

Worth is the achievement of learning outcomes school tuition in komulatif each semester . Cumulative is of daily on average the value of deuteronomy , deuteronomy the middle of the first half , but the end of the semester .The data the students were a form of important information received by students from the results of the process of learning and instruction , that is a good report card , the certificate , the value of deuteronomy everyday and so on .The scores students was also used to know which students at the time the occurrence of understanding the teaching process .Learning outcomes students was also much influenced by a number of factors of the internal and external case .Internal motions go factors, that is, derived from in an individual who learns , physical and spiritual example .The is a factor of its external who come from outside the individual itself , example the family , school , and the community.

On issues discussed, can apply design application data security is one of the algorithm markle hellman in securing the data. studentsTo secure the data is intended to help students the curriculum in securing the scores their students.

The research is the creation of an application security data with hellman markle algorithms that can help the curriculum in securing the scores of students.

Keywords : *Cryptography , markle hellman , and the value of the students*

1. PENDAHULUAN

Nilai adalah pencapaian hasil belajar peserta didik secara komulatif dalam satu semester. komulatif artinya perata-rataan dari rata-rata nilai ulangan harian, ulangan tengah semester, dan ulangan akhir semester.[1] Data nilai siswa adalah suatu bentuk informasi penting yang diterima oleh siswa dari hasil proses belajar dan pembelajaran, baik itu nilai rapor, ijazah, nilai ulangan sehari hari dan sebagainya.

Data nilai siswa juga digunakan untuk mengetahui sampai mana pemahaman siswa saat terjadinya proses pembelajaran. Hasil belajar siswa juga banyak dipengaruhi oleh beberapa faktor diantaranya faktor internal dan eksternal. Faktor internalnya yaitu faktor yang berasal dari dalam individu yang belajar,

contoh jasmani dan rohani. Sedangkan faktor eksternalnya adalah faktor yang berasal dari luar individu itu sendiri, contoh keluarga, sekolah, dan masyarakat.

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).[2] Kriptografi adalah suatu ilmu sekaligus seni yang bertujuan untuk menjaga keamanan suatu pesan (*cryptography is the art and science of keeping messages secure*).[3].

Merkle-Hellman *Knapsack* digunakan kunci privat dan kunci publik dalam melakukan proses kriptografinya, metode ini juga memiliki pengamanan ganda sehingga susah untuk ditembus.[4]
Berdasarkan masalah yang dihadapi, maka penulis mengangkat judul sebagai inti pembahasan dalam penelitian yaitu **"**Implementasi Kriptografi Merkle Hellman Dalam Mengamankan Data Nilai Siswa SMK Wira Kesuma Jaya Kec. Namo Rambe**"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

"Kriptografi berasal dari bahasa Yunani yaitu kripto yang artinya "*secret*" (rahasia) dan graphia yang artinya "*writting*" (tulisan). Menurut teminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan di kirim dari suatu tempat ke tempat yang lain"[5]. Contoh algoritma kriptografi yang dapat dihandalkan adalah Markle Hellman, dimana Markle Hellman merupakan kriptosistem yang menggunakan algoritma asimetris. 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).[6]

2.2 Markle Hellman

Algoritma Merkle-Hellman *Knapsack* merupakan kriprtosistem yang dibuat oleh Ralph Merkle dan Martin Hellman pada tahun 1978. Algoritma Merkle-Hellman *Knapsack* adalah algoritma kunci asimetris yang memiliki dua kunci yaitu *privatekey* dan *publickey*.[7]. Ide dasar di balik skema enkripsi Merkle-Hellman adalah menciptakan masalah subset yang bisa dipecahkan dengan mudah dan kemudian menyembunyikan sifat *superincreasing* dengan perkalian modular dan permutasi.

2.3 Algoritma Markle Hellman

Adapun algoritma penyelesaian metode Markle Hellman yaitu sebagai berikut:

1 Membuat *Private Key*.

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

2. Membuat *Public Key*.

Public Key digunakan untuk menghitung hasil *chipper* data. *Public key* memiliki karakter yang sama dengan *private key* S. 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*.

3. Merubah *Plaintext* Ke Binner Data 8 Digit

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

1. Menjumlahkan (Perkalian Binner Dengan *Public Key*).

Untuk proses perhitungan data *chipertext*, terlebih dahulu harus melakukan pembagian *plaintext* kedalam blok – blok berdasarkan jumlah elemen β. Diketahui jumlah elemen β sebanyak 8 elemen. Selanjutya, setiap blok akan dikaitkan dengan setiap elemen β, sihinngga diperoleh *chipertext*.

$C = \sum^{nj}_{=1} \alpha j \beta j$.....

2. Data *Chipherte*xt (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.

3. Modular *Invers.*
   Proses untuk mencari nilai modulo invers dari (P^{-1}) dengan menggunakan model *extended euledian*, yaitu (P * M mod A = 1).
4. Chipper Data Mod A.
   Proses berikutnya adalah proses mod, yaitu untuk data *chipertext* dengan nilai *invers* yang diperoleh sebelumnya.
5. 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 terjadi apabila kunci S tidak dibuat dengan metode *superincreasing linear*.

3. METODOLOGI PENELITIAN

Dalam melakukan sebuah penelitian ada beberapa cara yang dilakukan yaitu sebagai berikut :

1. *Data Collecting*

Dalam teknik pengumpulan data terdapat beberapa hal yang harus dilakukan di antaranya yaitu sebagai berikut:

a. Observasi
   Observasi merupakan salah satu kegiatan ilmiah empiris yang mendasarkan fakta – fakta lapangan maupun teks, melalui pengalaman panca indra tanpa menggunakan manipulasi.[8]
b. Wawancara
   Wawancara (interview) secara umum adalah suatu percakapan antara dua atau lebih orang yang dilakukanoleh pewawancara dan narasumber. Ada juga yang mengatakan bahwa definisi wawancara adalah suatu bentuk komunikasi lisan yang dilakukan secara terstruktur oleh dua orang atau lebih, baik secara langsung maupun jarak jauh. [9] .

2. Setudi Kepustakaan (*Library Search)*
   Teknik pengumpulan data yang digunakan pada dalam penelitian kepustakaan ini yaitu mencari data data mengenai hal hal atau variable berupa catatan, buku, makalah, artikel, jurnal, dan sebagainya (Arikunto & Jabar, 2010). [10].

3.1 Metode Perancangan Sistem

Berikut ini adalah teknik perancangan sistem yang digunakan adalah sebagai berikut :

1. Analisis Masalah dan Kebutuhan.
2. Perancangan Sistem dan Pemodelan.
3. Pengkodean.
4. Uji Coba Sistem
5. Implementasi Sistem

3.2 Algoritma Sistem

Algoritma sistem merupakan penjelasan langkah – langkah penyelesaian masalah dalam perancangan sistem Mengamankan Data Nilai Siswa dengan menggunakan algoritma Merkle Hellman, berikut ini adalah langkah-langkah penyelesaian metode Markle Hellman yaitu :

1. Membuat *Private Key*
2. Membuat *Public Key*.
3. Merubah *Plaintext* Ke Binner Data 8 Digit.
4. Menjumlahkan (Perkalian Binner Dengan *Public Key*).
5. Data *Chiphertex*t (C).
6. Modular *Invers.*
7. Chipper Data Mod A.
8. Mengurangkan Data Dengan Nilai S.

3.2.1 Penyelesaian

Berikut ini adalah data *Nilai Siswa* yang didapat dari SMK Wira Kesuma Jaya Kec. Namo Rambe, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:

Tabel 3.1 Sampel Data Nilai Siswa SMK Wira Kesuma Jaya Kec. Namo Rambe

Nama	Afni Berutu
Kelas	XI.IPA-2
Pelajaran	Fisika
UH1	88
UH2	90,00
UH3	91,00
Psikomotor1	86
Psikomotor2	84
UTS	86
UAS	86
NA	85,60

3.3.3 Penyelesaian Masalah Dengan Algoritma Markle Hellman.

Sesuai dengan referensi yang telah dipaparkan pada bab sebelumnya, berikut ini adalah langkah-langkah penyelesaiannya yaitu:

1. Proses Enkripsi Algoritma Rivest Shamir Adleman (RSA)

1. Membuat *Private Key*.
   Nilai S, P, A adalah *variable* untuk *private key*. Angka – angka bilangan bulat yang disusun dengan algoritma *superincreasing linear*. Nilai S terdiri dari beberapa angka tergantung dari jumlah digit binner yang digunakan. A adalah nilai (angka) bebas yang harus lebih besar dari jumlah keseluruhan nilai P. Sedangkan P adalah nilai (angka) bebas yang dapat diambil mulai dari angka 1sampai dengan A.

Tabel 3.2 *Private Key*

S	{2 , 4, 7, 14, 28, 112, 224, 407} $= \sum s = 798$
A	989
P	578

2. Membuat *Public Key*.
   Public Key digunakan untuk menghitung hasil *chipper* data. *Public key* memiliki karakter yang sama dengan *private key* S. 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*.

Tabel 3.3 *Public Key*

No	T = (P * Si) Mod A	
2	578 * 2 mod 989	167
4	578 * 4 mod 989	334
7	578 * 7 mod 989	90
14	578 * 14 mod 989	180
28	578 * 28 mod 989	360
112	578 * 112 mod 989	451
224	578 * 224 mod 989	902
407	578 * 407 mod 989	853

3. Merubah *Plaintext* Ke Binner Data 8 Digit
   Pada proses ini data perlu diubah menjadi bentuk binner karena perhitungan Merkle Hellman menggunakan teknik *binary* sebagai proses enkripsi dan deskripsinya. Untuk mengubah data ke

binary, maka sebelumnya data diubah ke kode ASCII. Langkah selanjutnya adalah mengubah kode ASCII tersebut menjadi *binary*.

Tabel 3.4 Data Binary Key

Plaintext	ASCII	Binary (Z)
8	56	00111000
8	56	00111000
Space	32	00111000
9	57	00111001
0	48	00110000
,	44	00101100
0	48	00110000
0	48	00110000
9	57	00111001
1	49	00110001
,	44	00101100
0	48	00110000
0	48	00110000
Space	32	00111000
8	56	00111000
6	54	00110110
Space	32	00111000
8	56	00111000
6	54	00110110
Space	32	00111000
8	56	00111000
4	52	00110100
Space	32	00111000
8	56	00111000
6	54	00110110
Space	32	00111000
8	56	00111000
6	54	00110110
Space	32	00111000
8	56	00111000
5	53	00110101
,	44	00101100
6	54	00110110
0	48	00110000
Space	32	00111000
8	56	00111000
6	54	00110110

3. Menjumlahkan (Perkalian Binner Dengan *Public Key*).

Untuk proses perhitungan data *chipertext*, terlebih dahulu harus melakukan pembagian *plaintext* kedalam blok – blok berdasarkan jumlah elemen β. Diketahui jumlah elemen β sebanyak 8 elemen. Selanjutya, setiap blok akan dikaitkan dengan setiap elemen β, sihinngga diperoleh *chipertext*.

Tabel 3.5 Data Perkalian Binner Dengan *Public Key*

Binary (Z)	$\sum z * Ti$	Chipertext
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630

00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111001	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(1*853)	1483
00110000	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(0*853)	270
00101100	(0*167)+(0*334)+(1*90)+(0*180)+ (1*360)+(1*451)+(0*902)+(0*853)	901
00110000	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(0*853)	270
00110000	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(0*853)	270
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111001	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(1*853)	1483
00110001	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(1*853)	1123
00101100	(0*167)+(0*334)+(1*90)+(0*180)+ (1*360)+(1*451)+(0*902)+(0*853)	901
00110000	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(0*853)	270
00110000	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(0*853)	270
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00110110	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(1*902)+(0*853)	1623
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00110100	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(0*902)+(0*853)	721
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00110110	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(1*902)+(0*853)	1623
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90

00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00110110	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(1*902)+(0*853)	1623
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00110101	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(0*902)+(1*853)	1574
00101100	(0*167)+(0*334)+(1*90)+(0*180)+ (1*360)+(1*451)+(0*902)+(0*853)	901
00110110	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(1*902)+(0*853)	1623
00110000	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(0*451)+(0*902)+(0*853)	270
00100000	(0*167)+(0*334)+(1*90)+(0*180)+ (0*360)+(0*451)+(0*902)+(0*853)	90
00111000	(0*167)+(0*334)+(1*90)+(1*180)+ (1*360)+(0*451)+(0*902)+(0*853)	630
00110110	(0*167)+(0*334)+(1*90)+(1*180)+ (0*360)+(1*451)+(1*902)+(0*853)	1623

Proses diatas menunjukkan bahwa proses enkripsi data sudah selesai dilakukan, proses enkripsi dari pesan (88 90,00 91,00 86 84 86 86 85,60 86) adalah
C = (630, 630, 90, 1483, 270, 901, 270, 270, 90, 1483, 1123, 901, 270, 270, 90, 630, 1623, 90, 630, 721, 90, 630, 1623, 90, 630, 1623, 90, 630, 1574, 901, 1623, 270, 90, 630, 1623).

2. Proses Dekripsi Algoritma Caesar Cipher

1. Data *Chiphertex*t (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.

C=(630,630,90,1483,270,901,270,270,90,1483,1123,901,270,270,90,630,1623,90,630,721,90,630,1623,90,630,1623,90,630,1574,901,1623,270,90,630,1623).

2. Modular *Invers.*

   Proses untuk mencari nilai modulo invers dari (P^{-1}) dengan menggunakan model *extended euledian*, yaitu (P * M mod A = 1). Dalam proses dekripsi ini akan digunakan nilai P^{-1} sebesar 77. Nilai 77 diperoleh dari hasil perhitungan metode *extended euledian*. Seperti tabeldi bawah ini :

Tabel 3.6 Modular *Invers*

M	P * M mod A	
1	578 * 1 mod 989	578
2	578 * 2 mod 989	167
3	578 * 3 mod 989	745
….	.... * …. mod 989	…..
77	57877 mod 989	1

3. Chipper Data Mod A.

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

Tabel 3.7 *Chiper* Data Mod A

Chiper (C)	**M**	**K = (C * M) mod A**	
630	77	630 * 989	49
630	77	630 * 989	49
90	77	90 * 989	7
1483	77	1483 * 989	456
270	77	270 * 989	21
901	77	901 * 989	147
270	77	270 * 989	21
270	77	270 * 989	21
90	77	90 * 989	7
1483	77	1483 * 989	456
1123	77	1123 * 989	428
901	77	901 * 989	147
270	77	270 * 989	21
270	77	270 * 989	21
90	77	90 * 989	7
630	77	630 * 989	49
1623	77	1623 * 989	357
90	77	90 * 989	7
630	77	630 * 989	49
721	77	721 * 989	133
90	77	90 * 989	7
630	77	630 * 989	49
1623	77	1623 * 989	357
90	77	90 * 989	7
630	77	630 * 989	49
1623	77	1623 * 989	357
90	77	90 * 989	7
630	77	630 * 989	49
1574	77	1574 * 989	540
901	77	901 * 989	147
1623	77	1623 * 989	357
270	77	270 * 989	21
90	77	90 * 989	7
630	77	630 * 989	49
1623	77	1623 * 989	357

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 terjadi apabila kunci S tidak dibuat dengan metode *superincreasing linear*.

S_1 = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_2 = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_3 = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_4 = 456 – 407 = 49 (1) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00111001**

S_5 = 21 – 407 = 0 (0) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 28 = 21(0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110000**

S_6 = 147 – 407 = 0 (0) | 147 – 224 = 0 (0) | 147 – 112 = 35 (1) | 35 – 28 = 7 (1) |7 – 14 = 0 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00101100**

S_7 = 21 – 407 = 0 (0) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 28 = 21(0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110000**

S_8 = 21 – 407 = 0 (0) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 28 = 21(0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110000**

S_9 = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{10} = 456 – 407 = 49 (1) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00111001**

S_{11} = 428 – 407 = 21 (1) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 0 = 21(0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110001**

S_{12} = 147 – 407 = 0 (0) | 147 – 224 = 0 (0) | 147 – 112 = 35 (1) | 35 – 28 = 7 (1) |7 – 14 = 0 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00101100**

S_{13} = 21 – 407 = 0 (0) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 28 = 21(0) | 21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110000**

S_{14} = 21 – 407 = 0 (0) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 28 = 21(0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110000**

S_{15} = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{16} = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_{17} = 357 – 407 = 0 (0) | 357 – 224 = 133 (1) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110110**

S_{18} = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{19} = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_{20} = 133 – 407 = 0 (0) | 133 – 224 = 0 (0) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110100**

S_{21} = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{22} = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_{23} = 357 – 407 = 0 (0) | 357 – 224 = 133 (1) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110110**

S_{24} = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{25} = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_{26} = 357 – 407 = 0 (0) | 357 – 224 = 133 (1) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110110**

S_{27} = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{28} = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_{29} = 540 – 407 = 133 (1) | 133 – 224 = 0 (0) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110101**

S_{30} = 147 – 407 = 0 (0) | 147 – 224 = 0 (0) | 147 – 112 = 35 (1) | 35 – 28 = 7 (1) |7 – 14 = 0 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00101100**

S_{31} = 357 – 407 = 0 (0) | 357 – 224 = 133 (1) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110110**

S_{32} = 21 – 407 = 0 (0) | 21 – 224 = 0 (0) | 21 – 112 = 0 (0) | 21 – 28 = 21(0) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110000**

S_{33} = 7 – 407 = 0 (0) | 7 – 224 = 0 (0) | 7 – 112 = 0 (0) | 7 – 28 = 21(0) |7 – 14 = 7 (0) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00100000**

S_{34} = 49 – 407 = 0 (0) | 49 – 224 = 0 (0) | 49 – 112 = 0 (0) | 49 – 28 = 21(1) |21 – 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00011100**

S_{35} = 357 – 407 = 0 (0) | 357 – 224 = 133 (1) | 133 – 112 = 21 (1) | 21 – 28 = 0 (0) |21– 14 = 7 (1) | 7 – 7 = 0 (1) | 0 – 4 = 0 (0) | 0 – 2 = 0 (0) = **00110110**

4. PEMODELAN SISTEM DAN PERANCANGAN

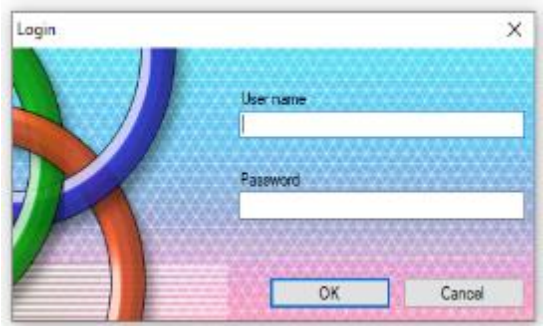
Pemodelan merupakan gambaran dari realita yang simple dan dituangkan dalam bentuk pemetaaan dengan aturan tertentu. Perancangan adalah usulan pokok yang mengubah sesuatu yang lebih baik, melalui tiga proses : mengidentifikasi masalah, mengidentifikasi mode untuk pemecahan masalah dan pelaksanaan pemecahan masalah. Berikut ini adalah penjelasan mengenai beberapa rancangan yang terdapat pada sistem berupa *use case diagram, activity diagram, dan class diagram*.

1. *Use Case Diagram*
   Sebuah *use case* diagram adalah diagram yang menggambarkan interaksi antara sistem eksternal dan pengguna
2. *Activity Diagram*
   Activity diagram adalah diagram yang menggambarkan suatu proses sistem berdasarkan *use case* diagram.
3. *Class Diagram*
   Class diagram adalah sebuah diagram yang digunakan unruk merancang bagaimana sistem dapat memiliki variable atau atribut penyimpan data beserta metode yang mendefinisikan cara data tersebut dikelola dalam sebuah sistem.

1. PENGUJIAN DAN IMPLEMENTASI

1. *Form Login*

Form Login digunakan untuk mengamankan sistem dari *user-user* yang tidak bertanggung jawab
sebelum masuk ke Menu Utama. Berikut adalah tampilan *Form Login* :



Gambar 1 *Form Login*

Berikut keterangan pada gambar 1 *Form Login* :

a. Tombol *OK* digunakan untuk mem-validasikan *username* dan *password* yang telah kita isi pada kotak teks yang disediakan.
b. Tombol *Cancel* digunakan ketika kita batal melakukan *login* dan akan keluar dari sistem..

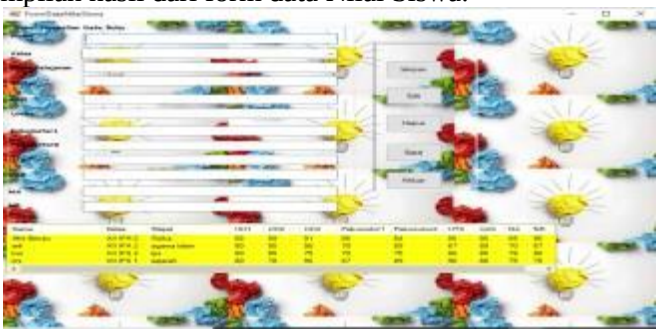
2. *Form* Menu Utama

Form Menu Utama digunakan sebagai penghubung untuk *Form* Data Nilai Siswa, *Form* Proses *Enkripsi*, *Form Dekripsi*, dan *Form* Laporan.

Gambar.2 *Form* Menu Utama

3. *Form* Data *Customer*

Berikut adalah tampilan hasil dari form data Nilai Siswa.



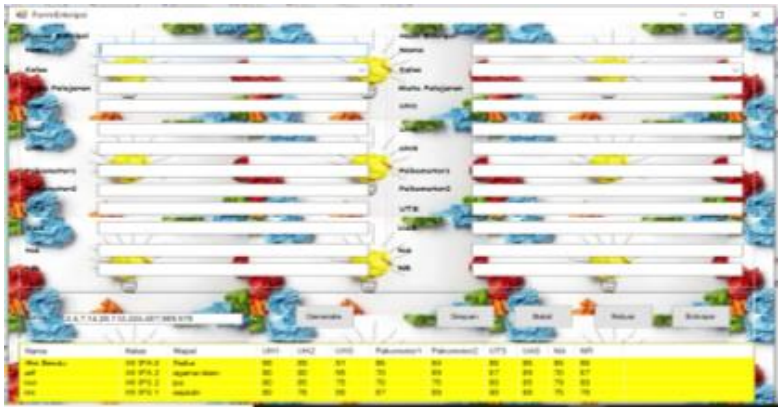
Gambar 3 *Form* Data Nilai Siswa

Berikut keterangan pada gambar 3 *form* Data *Customer*:

a. Tombol simpan digunakan ketika seluruh kotak teks telah terisi dan data dari kotak teks tersebut akan disimpan.
b. Tombol edit digunakan untuk mengubah data yang telah tersimpan sebelumnya.
c. Tombol hapus digunakan untuk menghapus data yang terpilih pada daftar data yang ada.
d. Tombol batal digunakan untuk membatalkan kegiatan saat mengubah data, menyimpan data dan sebagainya..
e. Tombol keluar digunakan untuk keluar dari form.

4. *Form* Enkripsi

Form Enkripsi adalah *Form* yang digunakan untuk Mengamankan data customer. Berikut adalah tampilan form Enkripsi:



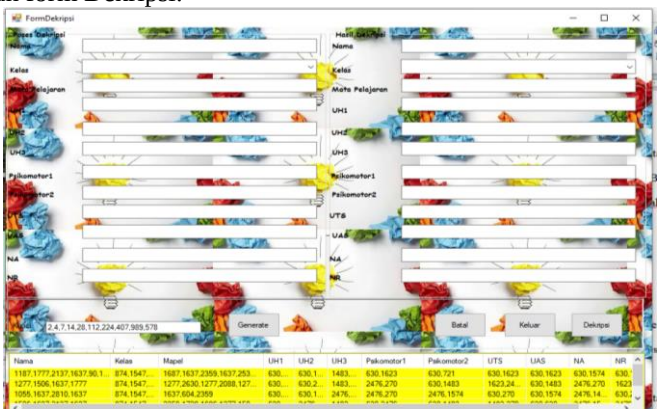
Gambar 4 *Form* Enkripsi

Berikut keterangan pada gambar 4 *form* Enkripsi:

a. Tombol Enkripsi digunakan untuk mengamankan data Nilai Siswa yang ada dengan menggunakan Markle Hellman.
b. Tombol key generator untuk mencari generator kunci yang lain.
c. Tombol Simpan digunakanuntuk menyimpan hasil enkripsi.
d. Tombol keluar digunakan untuk keluar dari form.
e. Tombol batal digunakan untuk membatalkan kegiatan saat menyimpan data dan sebagainya

5. *Form* Dekripsi

Form Dekripsi adalah *Form* yang digunakan untuk Mengubah data customer kembali seperti semula. Berikut adalah tampilan form Dekripsi:



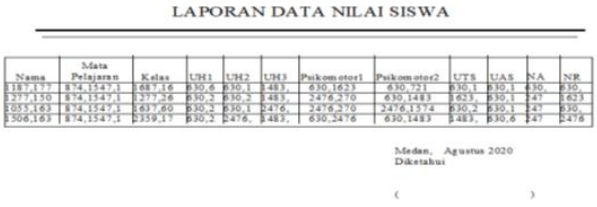
Gambar 5 *Form* Dekripsi

Berikut keterangan pada gambar 5 *form* Enkripsi:

a. Tombol Dekripsi digunakan untuk mengamankan data Nilai Siswayang ada dengan menggunakan Algoritma Markle Hellman.
b. Tombol key generator untuk mencari generator kunci yang lain.
c. Tombol Simpan digunakanuntuk menyimpan hasil enkripsi.
d. Tombol keluar digunakan untuk keluar dari form.
e. Tombol batal digunakan untuk membatalkan kegiatan saat menyimpan data dan sebagainya

6. *Form* Laporan

Form Laporan adalah *Form* yang digunakan untuk menampilkan hasil Enkripsi Data berdasarkan metode Markle Hellman. Berikut adalah tampilan form Laporan:



Gambar 6 *Form* Laporan

6. KESIMPULAN

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilalui dalam tahap perancangan dan evaluasi kriptografi dalam mengamankan data Nilai Siswa pada SMK WIRA KESUMA JAYA KEC. NAMO RAMBE dengan menggunakan algoritma Markel Hellman maka dapat disimpulkan bahwa:

1. Untuk mengamankan data Nilai Siswa SMK WIRA KESUMA JAYA KEC. NAMO RAMBE yang bersifat rahasia akan diamankan menggunakan algoritma kriptografi Markel Hellman.
2. Algoritma Markel Hellman digunakan sebagai sistem dalam pengamanan data yang merupakan algoritma yang cukup rumit dalam perhitungannya untuk mengamankan data yang cukup banyak sehingga dapat mengurangi resiko dalam penyalahgunaan data Nilai Siswa dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data Nilai Siswa SMK WIRA KESUMA JAYA KEC. NAMO RAMBE.
3. Dengan cara merancang sistem aplikasi yang dapat digunakan dalam mengamankan data Nilai Siswaa dan mengenkripsi data menjadi karakter sehingga dapat mengamankan data dengan maksimal dan baik.
4. Dengan sistem yang telah dibangun menggunakan aplikasi *Visual Studio* pada kriptografi dalam pengamanan data menggunakan algoritma Markel Hellman, Sehingga sistem ini mampu membantu dalam mengamankan data Nilai Siswa SMK WIRA KESUMA JAYA KEC. NAMO RAMBE .

REFERENSI

[1] S. Maria and I. Muawanah, "Perancangan Sistem Informasi Pengolahan Data Nilai Siswa Pada Sd Negeri 164 Pekanbaru," *J. Intra-Tech*, vol. 2, no. 1, pp. 1–11, 2018, [Online]. Available: file:///D:/Matakuliah Smstr 6/TA/PERANCANGAN SISTEM INFORMASI PENGOLAHAN DATA NILAI SISWA PADA SD NEGERI 164 PEKANBARU.pdf%0D.

[2] C. Science and I. Technology, "Implementasi kriptografi keamanan data resi pada pt jne perbaungan menggunakan metode merkle hellman," vol. 1, no. 1, pp. 6–10, 2020.

[3] A. P. N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *Jesik*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

[4] DediLeman, "Metode Merkle Hellman Untuk Enkripsi Dan Dekripsi Pesan Whatapp," *RiauJournalofComputerScience*, vol. 6, no. 1, pp. 45–49, 2020.

[5] B. Anwar, "Implementasi Metode Merkle Hellman Untuk Keamanan Informasi Daftar Pencarian Orang (DPO) Polda Sumatera Utara," no. 3, pp. 296–299, 2019.

[6] A. Hidayat, R. Rosyadi, and E. Paulus, "Aplikasi Merkle-Hellman Knapsack Untuk Kriptografi File Teks," vol. 2, no. November, pp. 26–27, 2016.

[7] A. Lestari, A. S. Sembiring, and T. Zebua, "Teknik Penyembunyian Pesan Teks Terenkripsi Algoritma Merkle-Hellman Knapsack Menggunakan Metode Pixel Value Differencing Ke Dalam Citra Digital," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 3, no. 1, pp. 204–212, 2019, doi: 10.30865/komik.v3i1.1590.

[8] H. Hasanah, "TEKNIK-TEKNIK OBSERVASI (Sebuah Alternatif Metode Pengumpulan Data Kualitatif Ilmu-ilmu Sosial)," *At-Taqaddum*, vol. 8, no. 1, p. 21, 2017, doi: 10.21580/at.v8i1.1163.

[9] A. N. Yuhana and F. A. Aminy, "Optimalisasi Peran Guru Pendidikan Agama Islam Sebagai Konselor dalam Mengatasi Masalah Belajar Siswa," *J. Penelit. Pendidik. Islam*, vol. 7, no. 1, p. 79, 2019, doi: 10.36667/jppi.v7i1.357.

[10] B. PERKEMBANGAN REMAJA Riskha Ramanda, Z. Akbar, and R. A. Murti Kusuma Wirasti, "Studi Kepustakaan Mengenai Landasan Teori Body Image," *J. EDUKASI J. Bimbing. Konseling*, vol. 5, no. 2, pp. 121–135, 2019.