International Journal of Artificial Intelegence Research ISSN:2579-7298
Vol 1, No 2, December 2017, pp.40 - 49

Application to Determination of Scholarship Worthiness Using Simple Multi Attribute Rating Technique and Merkle Hellman Method

Dicky Nofriansyah*, Ganefri, Sarjon Defit, Ridwan, Azanuddin, Haryo S Kuncoro
[1,4,5] Departement of Information System, STMIK Triguna Dharma
[1] Student Doctoral, Padang State University
[2] Rector of Padang State University, West Sumatera
[4] Lecturer of Padang State University, West Sumatera
[3] Rector of Universitas Putra Indonesia YPTK Padang, West Sumatera
Email: dicknofriansyah@ymail.com[1], ganefri_ft@yahoo.com[2] , sarjond@yahoo.co.uk[3] , azdin.bpc@gmail.com[4]

Article Info

Article history:

Received : 08/08/2017
Revised : 09/04/2017
Accepted : 10/04/2017

Keyword:

Decision Support System
Cryptography
Merkle Hellman
Simple Multi Attribute
Rating Technique

ABSTRACT

This research was focused on explaining how the concept of simple multi attribute rating technique method in a decision support system based on desktop programming to solve multi-criteria selection problem, especially Scholarship. The Merkle Hellman method is used for securing the results of choices made by the Smart method. The determination of PPA and BBP-PPA scholarship recipients on STMIK Triguna Dharma becomes a problem because it takes a long time in determining the decision. By adopting the SMART method, the application can make decisions quickly and precisely. The expected result of this research is the application can facilitate in overcoming the problems that occur concerning the determination of PPA and BBP-PPA scholarship recipients as well as assisting Student Affairs STMIK Triguna Dharma in making decisions quickly and accurately

I. INTRODUCTION

Decision Support System is an auxiliary tool for making decisions appropriately, and quickly. In Decision Support System can be applied several methods such as SMART Method (Simple Multi Attribute Rating Technique). The SMART method is a multi-criteria decision-making technique based on the theory. It has a weight that describes how important it is related to other criteria[1] [2] [3] [4] . This weighting is used to assess each alternative to obtain the best choice. In the problem discussed in this research, we will design a software using Desktop Programming which is expected to be a problem-solving solution and adopt Merkle Hellman Method as its data security. [2] [5] [6]

STMIK Triguna Dharma is one of the universities that receive the scholarship. The types of awards that are always accepted are classified as PPA Scholarships (Academic Achievement Improvement) and BBP-PPA (Educational Cost Assistance-Academic Achievement). Scholarship recipients must be following the criteria determined and selected in the selection process. During this selection process determination of scholarship recipients is still done conventionally, so that takes a long time. The problem of this selection process can be overcome by several ways one of them by using Decision Support System.

Desktop Programming is the software used to design a desktop-based system. The system will be designed to adopt the SMART Method and Merkle Hellman Method. In the concept of design is done by analysing the problems and needs in the issues discussed than done a rating of the causes of the reasons of the problem and in the final phase will be done a system design so that it can solve the problem as expected.

II. THEORY

a. Scholarship

The scholarship is a grant fee given to a person who is expected to help him finish his education to completion. For university students, Scholarship is divided into two, namely Academic Achievement Improvement Scholarship (PPA) and Tuition Fee Scholarship for Academic Achievement Improvement (BBP-PPA).

Awards for Academic Achievement Achievement and Educational Cost Assistance Improvement of Academic Achievement for Private Higher Education students is an effort of the government to provide encouragement and assistance to the students to follow their study smoothly and is expected to keep improving their academic achievement and to finish their education on time.

To provide Scholarship for Academic Achievement Improvement and Educational Cost Assistance, Academic Achievement Improvement can be made well following 3T principles, that is Right at Target, Exactly Amount, and Punctual. It takes technical means in assessing and selecting students who are entitled to get it. (BBP-PPA Scholarship Technical Guidelines: 2016)

b. Simple Multi Attribute Rating Technique

The techniques and steps in the SMART [3] [4] process, among others:

- Phase 1: Specify the number of criteria.
- Phase 2: Determine the criteria weights with the range of values 1-100 based on the importance of the criteria.
- Phase 3: Normalize the weighted value of the criteria by the formula $(w_j / \sum w_j)$,
- Phase 4: Provide a criteria value for each alternative.
- Phase 5: Calculate the utility value for each criterion by using the following formula:

$$u_i(a_i) = \frac{c_{out\,i} - c_{min}}{c_{max} - c_{min}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

c. Merkle Hellman

Cryptography is divided into two main processes namely the process of encryption and decryption; each process has a different algorithm[7]. Merkle Hellman method has several different calculations on the process of encryption and decryption[8]. At the time of the encryption process, the Merkle Hellman method uses the following model:

a. Encryption Process

$$c = \sum_{i=1}^{n} \propto_i \beta_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Phase 1: Create a Private Key (S, A and P)

The S, A, and P values are the variables for the private key. The integer numbers are arranged with linear superincreasing algorithms. S consists of several numbers depending on the number of binner digits used. A is a free value (figure) that must be greater than the total value of S with a maximum value of 999. While P is a free (number) value that can be taken starting from 1 to A.

$$A > \sum_{i=1}^{n} w_i \quad \ldots\ldots\ldots\ldots\ldots (3)$$

Phase 2: Create a Public Key

The public key is used to calculate the result of Cipher data. The public key has the same character as the private key S. If S denotes the private key, then the public key can be denoted by T. The public key has a row of numbers as the key to finding the Cipher[9] [10].

Phase 3: Changing Plaintext to Binner 8 Digit

Process of the data needs to be converted into binner form because Merkle Hellman calculation uses binary technique as encryption and decryption process. To convert data to binary 8 digits, then previous data is changed to ASCII code. The next step is to convert the ASCII code into an 8-digit binary code like below[8]:

Phase 4: Summing (Multiplication Binner with Public Key)

For the process of calculating the data of the Cipher text, must first do the plaintext division into blocks based on the number of elements T. Known the number of elements of T as many as 8 elements. Furthermore, each block will be associated with each element of T.

b. Decryption Process

During the decryption process, Merkle Hellman method uses the following model.

$$c' = \sum_{i=1}^{n} \propto_i w_i \quad \ldots\ldots\ldots\ldots (4)$$

The steps in the decryption process using the Merkle Hellman method is as follows:

Phase 1: Ciphertext Data (O)

In doing the decryption process, there must first be a complete data from the encryption process. It is necessary also a private key as a key to the process of data decryption.

Phase 2: Modular Invers

The process for finding the inverse modulo value of (p-1) using the extended eucledian method, ie (P * M mod A = 1). In this decryption process will be used p-1 value of 77. Value 77 obtained from the calculation using the method of extended eucledian.

Phase 3: Cipher Data Mod A

The next process is the modif process, which is for the data Ciphertext with the inverse value obtained previously

Phase 4: Reduce Data with Value S

The data reduction process (K) with the values of the S. The elements of decline continue from the largest to the smallest detail. The final result of the deduction must be a value of 0. The final result where the reduction is nonzero, the decryption process is declared to fail. The cause of failure can occur if the S key is not made by the linear superincreasing method.

Phase 5: Return to Original Data

Reverting to original data is the last step to convert to decryption process. The binary code is compiled and converted to decimal code then to char code

III. ANALYSIS AND DESIGN

3.1 Concept of Simple Multi Attribute Rating Technique

After conducting interviews with parties involved in the process of determining the PPA and BBP-PPA scholarship recipients on STMIK Triguna Dharma, there are some important things that can be taken as material criteria for the development of Decision Support System, i.e., data in the form of measures needed during the process of awarding the scholarship recipient. The criteria for the PPA and BBP-PPA scholarship are different, and the difference lies in the weight and number of measures required.

In the PPA award, the necessary criteria are GPA, Certificate - SK and Achievement. While on BBP-PPA scholarship, the required standards are Parent Income, Certificate - SK and Achievement. The weight of each criterion is determined by the Head of Student Affairs of STMIK Triguna Dharma, where the weight is determined based on the importance level as the reference of the students' worthiness assessment. Range assessment criteria between 0 - 100. Students will be sorted based on the highest to lowest score and will be passed from the highest to the lowest to meet the number of quotas that has been determined by Kopertis Region 1

Table 1. Quota of Scholarship

No	Scholarship	Quota
1	PPA	7
2	BBP – PPA	5

The data of the enrolled students are separated by their respective groups, namely the PPA scholarship group and the BBP-PPA scholarship group. Student data can be seen in the table below. Utility values are obtained by using a predetermined formula. The minimum value of criteria for each alternative is 0 (zero) and a maximum of 4 (four). Here is the process of calculating utility values:

a. Encryption Process

Phase 1: Calculation of Utility Candidate Value of PPA Candidate

- $U(2013020231_{P1}) = \frac{3.82 - 0}{4 - 0} = 0.955$
- $U(2013020419_{P1}) = \frac{3.79 - 0}{4 - 0} = 0.948$
- $U(2013020704_{P1}) = \frac{3.73 - 0}{4 - 0} = 0.933$
- $U(2015020878_{P1}) = \frac{3.91 - 0}{4 - 0} = 0.978$
- $U(2013030038_{P1}) = \frac{3.75 - 0}{4 - 0} = 0.938$
- $U(2014021130_{P1}) = \frac{3.74 - 0}{4 - 0} = 0.935$
- $U(2013020445_{P1}) = \frac{3.77 - 0}{4 - 0} = 0.943$
- $U(2013020900_{P1}) = \frac{3.73 - 0}{4 - 0} = 0.933$
- $U(2013020053_{P1}) = \frac{3.73 - 0}{4 - 0} = 0.933$
- $U(2015020667_{P1}) = \frac{3.91 - 0}{4 - 0} = 0.978$
- $U(2013020231_{P2}) = \frac{2 - 0}{4 - 0} = 0.500$
- $U(2013020419_{P2}) = \frac{2 - 0}{4 - 0} = 0.500$
- $U(2013020704_{P2}) = \frac{3 - 0}{4 - 0} = 0.750$
- $U(2015020878_{P2}) = \frac{1 - 0}{4 - 0} = 0.250$
- $U(2013030038_{P2}) = \frac{3 - 0}{4 - 0} = 0.750$
- $U(2014021130_{P2}) = \frac{1 - 0}{4 - 0} = 0.250$
- $U(2013020445_{P2}) = \frac{3 - 0}{4 - 0} = 0.750$
- $U(2013020900_{P2}) = \frac{2 - 0}{4 - 0} = 0.500$
- $U(2013020053_{P2}) = \frac{3 - 0}{4 - 0} = 0.750$
- $U(2015020667_{P2}) = \frac{1 - 0}{4 - 0} = 0.250$

- U(2013020231 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020419 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020704 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2015020878 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013030038 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2014021130 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020445 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020900 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020053 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$
- U(2015020667 $_{P3}$) = $\frac{1-0}{4-0} = 0.250$

Phase 2: Calculation of Utility Candidate Value of BBP-PPA Receiver

- U(2013020358 $_{B1}$) = $\frac{4-0}{4-0} = 1.000$
- U(2013020549 $_{B1}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020123 $_{B1}$) = $\frac{4-0}{4-0} = 1.000$
- U(2015020442 $_{B1}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020103 $_{B1}$) = $\frac{4-0}{4-0} = 1.000$
- U(2014020481 $_{B1}$) = $\frac{4-0}{4-0} = 1.000$
- U(2013020605 $_{B1}$) = $\frac{3-0}{4-0} = 0.750$
- U(2013020096 $_{B1}$) = $\frac{2-0}{4-0} = 0.500$
- U(2014020580 $_{B1}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020038 $_{B1}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020358 $_{B2}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020549 $_{B2}$) = $\frac{4-0}{4-0} = 1.000$
- U(2013020123 $_{B2}$) = $\frac{0-0}{4-0} = 0.000$
- U(2015020442 $_{B2}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020103 $_{B2}$) = $\frac{1-0}{4-0} = 0.250$
- U(2014020481 $_{B2}$) = $\frac{1-0}{4-0} = 0.250$
- U(2013020605 $_{B2}$) = $\frac{3-0}{4-0} = 0.750$
- U(2013020096 $_{B2}$) = $\frac{1-0}{4-0} = 0.250$
- U(2014020580 $_{B2}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020038 $_{B2}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020358 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2013020549 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2013020123 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2015020442 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2013020103 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2014020481 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2013020605 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2013020096 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$
- U(2014020580 $_{B3}$) = $\frac{2-0}{4-0} = 0.500$
- U(2013020038 $_{B3}$) = $\frac{0-0}{4-0} = 0.000$

The final calculation is the calculation of the utility value with the criterion weight. After the calculation results obtained for each criterion, then add the total value of each criterion to get the total. The total value becomes the final value for each alternative, and this value will be sorted by the highest value.

Phase 3: Result of Final Counting and Ranking

Students who are graduated are students who have final grade results starting from the highest to the lowest based on the number of quota of scholarship recipients that have been determined. The number of PPA scholarship recipients is 7 (seven) people, and BBP-PPA scholarship recipients are 5 (five) persons.

3.2 Concept of Merkle Hellman

Securing scholarship data recipients is considered important so that data is encrypted and can not be manipulated by people who intend badly. The data of the scholarship recipient is only visible to the person who has the authority. In this case, the person is the Head of Student Affairs STMIK Triguna Dharma. Merkle Hellman's security measures are as follows. The steps of the encryption process are as follows:

Phase 1: Create a Private Key (S, A, and P)

The S, A, and P values are the variables for the private key. The integer numbers are arranged with linear superincreasing algorithms. S consists of several numbers depending on the number of binner digits used. A is a free value (figure) that must be greater than the total value of S with a maximum value of 999. While P is a free (number) value that can be taken starting from 1 to A.

Table 2: Private Key

S	**{2, 4, 7, 14, 28, 112, 224, 407} = ∑s = 798**
A	989
P	578

Phase 2: Create a Public Key

A public key is used to calculate the result of Cipher data. The public key has the same character as the private key S. If the private key is denoted by S, then the public key can be denoted by T. Therefore the public key has a row of numbers as the key to finding the Cipher. Calculation of public key as the table below:

Table 3: Public Key

S	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

Phase 3: Changing Plaintext to Binner 8 Digit

In this process, the data needs to be converted into binner form because Merkle Hellman calculation uses a binary technique as encryption and decryption process. To convert data to binary 8 digits, then previous data is changed to ASCII code. The next step is to convert the ASCII code into an 8-digit binary code like below:

Table 4: Data Binary

Alphabet	ASCII	Binary (Z)
2	050	00110010
0	048	00110000
1	049	00110001
3	051	00110011
0	048	00110000
2	050	00110010
0	048	00110000
2	050	00110010
3	051	00110011
1	049	00110001

Phase 4: Summing (Multiplication Binner with Public Key)

For the process of calculating the data of the ciphertext, must first do the plaintext division into blocks based on the number of elements T. Known the number of elements of T as many as 8 elements. Next, each block will be associated with each element T, so the ciphertext obtained as follows:

Table 5: Result

Binary	Σz * T	*Chippertext*
00110010	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(1*902)+(0*853)	1172
00110000	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(0*902)+(0*853)	270
00110001	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(0*902)+(1*853)	1123
00110011	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(1*902)+(1*853)	2025
00110000	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(0*902)+(0*853)	270
00110010	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(1*902)+(0*853)	1172
00110000	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(0*902)+(0*853)	270
00110010	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(1*902)+(0*853)	1172
00110011	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(1*902)+(1*853)	2025
00110001	(0*167)+(0*334)+(1*90)+(1*180)+(0*360)+(0*451)+(0*902)+(1*853)	1123

The above process shows that the data encryption process is done. The last thing to do is to present the Ciphertext data by saving it back into text form. So the result of Encryption process of message 2013020231 is C {1172, 270, 1123, 2025, 270, 1172, 270, 1172, 2025, 1123}.

b. Decryption Proces

Steps in the decryption process using Merkle Hellman method are as follows:

Phase 1: Ciphertext Data (O)

In doing the decryption process, there must first be a complete data from the encryption process. In addition it is necessary also a private key as a key to the process of data decryption.

The Ciphertext code is as follows: C {1172, 270, 1123, 2025, 270, 1172, 270, 1172, 2025, 1123}.

Phase 2. Modular Invers

The process for finding the inverse modulo value of (p-1) using the extended eucledian method, ie (P * M mod A = 1). In this decryption process will be used p-1 value of 77. Value 77 obtained from the calculation using the method of extended eucledian, as the table below:

Table 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
…	…	…
77	578 * 77 mod 989	1

Phase 3. Cipher Data Mod A

The next process is the modif process, which is for the data Ciphertext with the inverse value obtained previously

Table 7. Cipher Data Mod A

O	M	(O*M) Mod A	
1172	77	1172 * 77 mod 989	245
270	77	270 * 77 mod 989	21
1123	77	1123 * 77 mod 989	428
2025	77	2025 * 77 mod 989	652
270	77	270 * 77 mod 989	21
1172	77	1172 * 77 mod 989	245
270	77	270 * 77 mod 989	21
1172	77	1172 * 77 mod 989	245
2025	77	2025 * 77 mod 989	652
1123	77	1123 * 77 mod 989	428

Phase 4. Reduce Data with Value S

The data reduction process (K) with the values of the S. elements The reduction continues from the largest to the smallest element. The final result of the deduction must be a value of 0. The final result where the reduction is nonzero, the decryption process is declared to fail. The cause of failure can occur if the S key is not made by the linear siperincreasing method. S = {2, 4, 7, 14, 28, 112, 224, 407}, K = {245, 21, 428, 652, 21, 245, 21, 245, 652, 428}

Table 8. Data Reduction Process

2	4	7	14	28	112	224	407	S
							245-407	K
						245-224		
					21-112	=21		
				21-28				
			21-14					
		7-7	=7					
	0-4	=0						
0-2								
0	**0**	**1**	**1**	**0**	**0**	**1**	**0**	

The calculation process in the above table starts from right to left, the column that is marked false means that on the element S column the data can not be subtracted and will be false or 0. While the column that contains the data true, means the data can be subtracted and true or 1 If the result of the data is taken entirely it will generate value "00110010" which if returned to the decimal code to "50" and to char to "2". The next process, the values V1 to V10 will decomposition use each value on S. This decomposition is done by subtracting the largest value to the smallest and yielding the value Vi = 0.

V1 = 245 - 407 = 245 (0) | 245 - 224 = 21 (1) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained result = 00110010

V2 = 21 - 407 = 21 (0) | 21 - 224 = 21 (0) | 21 - 112 = 21 (0) | 21 - 28 = 21 (0) |
21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained the result = 00110000

V3 = 428 - 407 = 21 (1) | 21 - 224 = 21 (0) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then the results obtained = 00110001

V4 = 652 - 407 = 245 (1) | 245 - 224 = 21 (1) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained the result = 00110011
V5 = 21 - 407 = 21 (0) | 21 - 224 = 21 (0) | 21 - 112 = 21 (0) | 21 - 28 = 21 (0) |
21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained the result = 00110000
V6 = 245 - 407 = 245 (0) | 245 - 224 = 21 (1) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained result = 00110010
V7 = 21 - 407 = 21 (0) | 21 - 224 = 21 (0) | 21 - 112 = 21 (0) | 21 - 28 = 21 (0) |
21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained the result = 00110000
V8 = 245 - 407 = 245 (0) | 245 - 224 = 21 (1) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained result = 00110010
V9 = 652 - 407 = 245 (1) | 245 - 224 = 21 (1) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)

Then obtained the result = 00110011
V10 = 428 - 407 = 21 (1) | 21 - 224 = 21 (0) | 21 - 112 = 21 (0) |
21 - 28 = 21 (0) | 21 - 14 = 7 (1) | 7 - 7 = 0 (1) | 0 - 4 = 0 (0) | 0 - 2 = 0 (0)
Then the results obtained = 00110001

Z = {00110010, 00110000, 00110001, 00110011, 00110000, 00110010, 00110000, 00110010, 00110011, 00110001}

Phase 5. Return to Original Data

Reverting to original data is the last step to convert to decryption process. The binary code is compiled and converted to decimal code then to char code.
C = C {1172, 270, 1123, 2025, 270, 1172, 270, 1172, 2025, 1123}
Z = {2013020231}

c. Simulation

System test aims to prove that the input, process, output generated by Visual Basic.Net 2008 system application system has been correct and following the desired. Testing the system by entering data into the system and pay attention to the output generated. If the input, process, and output are appropriate, then the system is correct. Stages of testing the system as follows:

a. Perform input data criteria,
b. Show information quota data,
c. Conducting student data input,
d. Indicating the process of appraising prospective scholarship students by applying the SMART Method,

e. Conduct encryption and decryption test on learning data. Encryption is done when saving data into the database. While Decryption is done when displaying the report of the scholarship recipient.

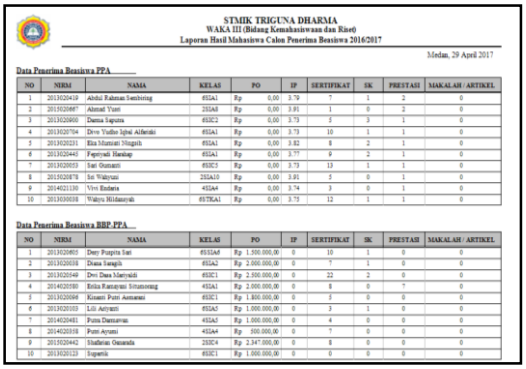
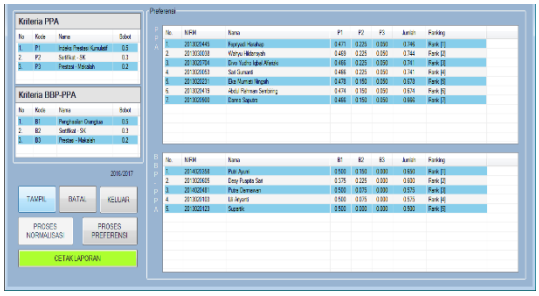


Figure 1: Learning Data

The report of the scholarship recipients is used to display the data of the students who are selected to be the recipients of the award using Simple Multi Attribute Rating Technique.

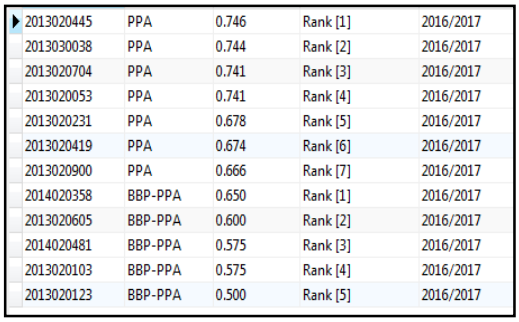
Figure 2: Application of Scholarship Using



SMART

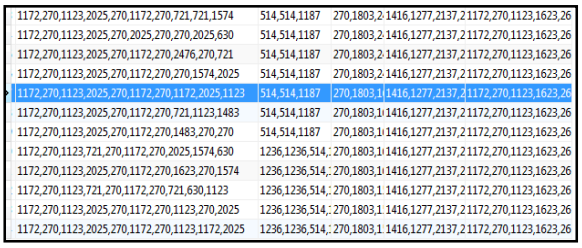
The following is the result of system testing that has been made based on the results of the analysis manually:
Result of Determination Test of Scholarship Recipient. Below is the data of PPA and BBP-PPA scholarship recipients are stored in the database.

Figure 3: Data of Scholarship in Database



2013020445	PPA	0.746	Rank [1]	2016/2017
2013030038	PPA	0.744	Rank [2]	2016/2017
2013020704	PPA	0.741	Rank [3]	2016/2017
2013020053	PPA	0.741	Rank [4]	2016/2017
2013020231	PPA	0.678	Rank [5]	2016/2017
2013020419	PPA	0.674	Rank [6]	2016/2017
2013020900	PPA	0.666	Rank [7]	2016/2017
2014020358	BBP-PPA	0.650	Rank [1]	2016/2017
2013020605	BBP-PPA	0.600	Rank [2]	2016/2017
2014020481	BBP-PPA	0.575	Rank [3]	2016/2017
2013020103	BBP-PPA	0.575	Rank [4]	2016/2017
2013020123	BBP-PPA	0.500	Rank [5]	2016/2017

Below is the data of the scholarship recipient in the encrypted database. Examples of cases of encrypted data are:
Plaintext = {2013020231}
Chipper = {1172, 270, 1123, 2025, 270, 1172, 270, 1172, 2025, 1123}



1172,270,1123,2025,270,1172,270,721,721,1574	514,514,1187	270,1803,2·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,2025,270,270,2025,630	514,514,1187	270,1803,2·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,2476,270,721	514,514,1187	270,1803,2·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,270,1574,2025	514,514,1187	270,1803,2·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,1172,2025,1123	514,514,1187	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,721,1123,1483	514,514,1187	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,1483,270,270	514,514,1187	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,721,270,1172,270,2025,1574,630	1236,1236,514,:	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,1623,270,1574	1236,1236,514,:	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,721,270,1172,270,721,630,1123	1236,1236,514,:	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,1123,270,2025	1236,1236,514,:	270,1803,1·1416,1277,2137,21172,270,1123,1623,26
1172,270,1123,2025,270,1172,270,1123,1172,2025	1236,1236,514,:	270,1803,1·1416,1277,2137,21172,270,1123,1623,26

Figure 4: Ciphertext of Data Scholarship Using Merkle Hellman Algorithm

III. CONCLUSION

The conclusion of this research is Simple Multi Attribute Rating Technique method can be used to determine the eligibility of the scholarship recipient and the result of the method is then re-secured using Merkle Hellman method to maintain data integrity.

IV. REFERENCE

[1] D. Nofriansyah, *Konsep Data Mining Vs Sistem Pendukung Keputusan*. Yogyakarta: CV. Deepublish, 2014.

[2] D. Nofriansyah, "COMBINATION OF PIXEL VALUE DIFFERENCING ALGORITHM WITH CAESAR ALGORITHM FOR STEGANOGRAPHY," *International Journal of Research In Science & Engineering*, vol. 2, 2016.

[3] F. H. Barron and B. E. Barrett, "The efficacy of SMARTER — Simple Multi-Attribute Rating Technique Extended to Ranking," *Acta Psychologica*, vol. 93, pp. 23-36, 1996/09/01/ 1996.

[4] C. S. Yap, *et al.*, "Methods for information system project selection: an experimental study of AHP and SMART," in *Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences*, 1992, pp. 578-589 vol.3.

[5] A. Sridhar and V. R. Josna, "CASH on Modified Elgamal: A Preventive Technique for False Channel Condition Reporting Attackin Ad-hoc Network," *Procedia Technology*, vol. 24, pp. 1276-1284, 2016/01/01/ 2016.

[6] S. Yuan, *et al.*, "Cryptanalysis and security enhancement of optical cryptography based on computational ghost imaging," *Optics Communications*, vol. 365, pp. 180-185, 2016/04/15/ 2016.

[7] K. Marisa W. Paryasto, Sarwan et al, "Issues in Elliptic Curve Crypyography implementation," *Internetworking Indonesial Journal*, vol. 1, 2009.

[8] G. Lokeshwari, Aparna, G., & Dr. Udaya Kumar, S, "A Novel Scheme for Image Encryption using Merkle-Hellman Knapsack Cryptosystem-Approach, Evaluation and Experimentation," *International Journal of Computer Science & Technology*, vol. 2, 2011.

[9] L. Ogiela, "Cryptographic techniques of strategic data splitting and secure information management," *Pervasive and Mobile Computing*, vol. 29, pp. 130-141, 2016/07/01/ 2016.

[10] A. S. N. C. A. Rama Krishna , A. S. C. S. Sastry, "A Hybrid Cryptographic System for Secured Device to Device Communication," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, 2016.